

TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Eraõiguse instituut

Merle Peeterson

TÖÖTAJA PRIVAATSUSÕIGUS JA SELLE PIIRAMINE TÖÖSUHETES

Magistritöö

Juhendaja
dr iur Gaabriel Tavits

Tallinn
2012

SISUKORD

SISSEJUHATUS	4
1. TÖÖTAJA ÕIGUS PRIVAATSUSELE	8
1.1 Privaatsuse ja privaatsusõiguse määratlemine.....	8
1.1.1 Õigus vabale eneseteostusele.....	12
1.1.2 Õigus eraelu puutumatusel.....	13
1.1.3 Õigus sõnumisaladusele	14
1.1.4 Õigus väljendusvabadusele	16
1.2 Töötaja põhiõigustele vastanduvad tööandja põhiõigused	17
1.2.1 Ettevõtlusvabadus	18
1.2.2 Omandipõhiõigus	18
1.3 Privaatsusõiguse kui põhiõiguse riive lubatavus ja proportsionaalsus.....	19
2. ISIKUANDMETE TÖÖTLEMINE TÖÖSUHETES	22
2.1 Isikuandmete töötlemise ja selle piiramise vajalikkus	22
2.2 Isikuandmete töötlemise põhimõisted	24
2.3 Isikuandmete töötlemise õiguslikud alused	25
2.3.1 Seadusest tulenevad alused.....	26
2.3.2 Töötlemine töötaja nõusolekul	27
2.4 Isikuandmete töötlemise põhimõtted.....	28
2.5 Tööandja vastutus isikuandmete töötlemisel.....	33
2.5.1 Andmekaitse Inspeksiooni poolt kohaldatavad sanktsioonid.....	34
2.5.2 Töötajapoolne töölepingu erakorraline ülesütlemine ja kahju hüvitamine	35
2.5.3 Karistusõiguslik vastutus.....	37
3. TÖÖTAJA PRIVAATSUSE PIIRAMINE TÖÖSUHETES.....	40
3.1 Töötaja kontrollimine	40
3.1.1 Töötaja kontrollimise meetodid.....	42
3.1.2 Delikaatsed isikuandmed töötaja kontrollimisel.....	44
3.1.2.1 Joobeseisund.....	44
3.1.2.2 Ajutine töövõimetus	47
3.1.2.3 Tervisekontroll	48
3.2 Kommunikatsioonivahendite kasutamise jälgimine.....	50
3.2.1 E-kirjad	52
3.2.2 Internet.....	56
3.2.3 Telefon.....	59

3.2.4 Kommunikatsioonivahendite kasutamise reeglid.....	61
3.3 Jälgimisseadmete kasutamine.....	64
KOKKUVÕTE	70
EMPLOYEE´S RIGHT TO PRIVACY AND ITS RESTRICTION IN LABOUR RELATIONS. SUMMARY	74
KASUTATUD LÜHENDID	80
KASUTATUD KIRJANDUS	81
KASUTATUD ÕIGUSAKTID	84
KASUTATUD KOHTUPRAKTIKA	85

SISSEJUHATUS

Õigus privaatsusele on üks olulisemaid ja delikaatsemaid põhiõigusi, mis puudutab igäht, kuna kõigil on isiklik elu, millest kindlasti nii mõndagi ei olda nõus valimatult teiste inimestega jagama. Seni, kuni seda hüve ei riivata, inimesed oma privaatsusõigusele sageli ei mõtle. Privaatsus ja õigus privaatsusele satub tähelepanu alla reeglina siis, kui keegi seda õigushüve ohustab. Paraku loob infotehnoloogia kiire ja pidev areng aina juurde võimalusi privaatsuse riiveks ning seetõttu on privaatsuse ja selle kaitsmise teema järjest rohkem päevakorral. Erialakirjanduses on avaldatud isegi arvamust, et privaatsust ei olegi enam olemas, kuna kaasaegsed infotehnoloogilised lahendused võimaldavad inimesi jälgida sisuliselt igal pool, või on leitud, et privaatsuse tähendus on muutunud, kuna see ei ole enam inimestele nii oluline kui enne.¹ Kindlasti on privaatsuse tähendus aja jooksul inimeste jaoks mingil määral muutunud, kuid pidevalt kasvav eraellu liigse sekkumise oht on pigem pannud inimesi privaatsust rohkem hindama ning oma privaatsusõigusele kaitset otsima.

Kuigi inimeste vajadus privaatsuse järele ning privaatsuse tunnetus on väga erinev, siis teatud privaatsust eeldatakse tegelikult igal ajal ja igal pool, kuid olenevalt kohast ja olukorrast on oodatav privaatsuse tase erinev. Kui oma kodus on ootused privaatsusele ja privaatsusõiguse tagamisele eriti kõrged, siis näiteks tänaval või mõnel avalikul üritusel osaledes on need ootused tunduvalt väiksemad, kuid mingil määral on need ka siis ikkagi olemas. Töökoht, kus enamus tööealisi inimesi veedavad suure osa oma ajast, jääb nimetatud kahe äärmuse vahele. Võrreldes avalikus kohas viibimisega, eeldatakse töökohal kindlasti tunduvalt suuremat privaatsust. Kuigi tänapäeval on töö- ja eraelu ühene eristamine järjest keerulisem, ei saa töötajad eeldada töökohal siiski samasugust privaatsust kui oma kodus. Seda juba seetõttu, et töösuhetes on kaks poolt – töötaja ja tööandja ning seega tuleb arvestada ka tööandja õiguste ja huvidega, mis teatud olukordades vastanduvad töötaja õigustele ja huvidele. Üheks selliseks juhuks on töötaja privaatsusõiguse vastandumine tööandja põhiõigustega – ettevõtlusvabaduse ja omandipõhiõigusega. Töötajal on õigus oma privaatsuse kaitsele, samas on tööandjal aga õigus kaitsta oma majanduslikke huve.

Käesolev magistritöö käsitleb töötaja privaatsusõigust ning selle piiramist töösuhetes, seda eelkõige läbi töötaja kontrollimise ja kommunikatsioonivahendite kasutamise jälgimise, mis teatud juhtudel võivad töötaja privaatsusõigust tõsiselt riivata. Töölepingu seaduse² (edaspidi

¹ M.R.Dowding. Privacy: Defending an Illusion. Plymouth: Scarecrow Press 2011, lk V.

² Töölepingu seadus. – RT I 2009, 5, 35 ... RT I, 10.02.2012, 2.

TLS) §-i 1 kohaselt allub töötaja tööandja juhtimisele ja kontrollile. Samas tuleb seda kontrolli teostada nii, et austatakse töötaja privaatsust ega rikutaks tema põhiõigusi. Eelnevast tulenevalt on käesoleva magistritöö eesmärgiks välja selgitada, millistel juhtudel, millises ulatuses ja millisel viisil võib tööandja töötaja privaatsusõigust piirata, näiteks lindistada telefonikõnesid, lugeda töötaja e-kirju, jälgida töötaja arvutikasutamist, filmida töötajaid turvakaameratega või jälgida ja kontrollida töötajaid muude meetodite abil. Lisaks uuritakse magistritöös, kas sellist kontrollimist ja jälgimist oleks vaja seadusandja poolt täpsemalt reguleerida.

Teema on aktuaalne, kuna hetkel Eestis töötajate privaatsusõiguse piiramise kohta töösuhetes konkreetne seaduslik regulatsioon puudub, sest Eestis ei ole eriseadust, mis reguleeriks andmekaitset töösuhetes. Kuna töötajate jälgimine ja kontrollimine tööandja poolt kujutab endast isikuandmete töötlemist, siis tuleb antud küsimustes lähtuda üldistest isikuandmete töötlemise ja kaitse põhimõtetest, mis on sätestatud isikuandmete kaitse seaduses³ (edaspidi IKS). Andmekaitse teema üldiselt on päevakorral kogu Euroopa Liidus. Seoses sellega, et tehnoloogia kiire areng on põhjustanud uusi probleeme isikuandmete kaitse valdkonnas, jagatavate ja kogutavate andmete maht on oluliselt suurenenud ning tehnoloogia võimaldab nii eraettevõtetal kui ka riigiasutustel kasutada isikuandmeid enneolematult laias ulatuses oma tegevuse elluviimiseks, siis kavandatakse isikuandmete kaitseks uut õiguslikku raamistikku, mille osaks on ka Euroopa Parlamendi ja nõukogu määruse eelnõu üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus).⁴

Teema olulisusest ühiskonnas annab märku ka see, et töötaja kommunikatsioonivahendite jälgimist puudutavad küsimused on leidnud korduvalt kajastamist meediaväljaannete vahendusel. Samuti viitab probleemi olemasolule ja aktuaalsusele see, et Andmekaitse Inspeksioon on pidanud vajalikuks anda 2011. aasta alguses välja juhendmaterjali „Isikuandmete töötlemine töösuhetes“⁵ (edaspidi AKI juhise), milles muuhulgas on leidnud põhjalikumalt käsitlemist ka töötajate kontrollimise ja jälgimise teema. Samas on AKI juhise järgimine tööandjale soovituslik. Seega püütakse käesolevas töös ka välja selgitada, kas

³ Isikuandmete kaitse seadus. – RT I 2007, 24, 127 ... RT I, 30.12.2010, 11.

⁴ Seletuskiri Euroopa Parlamendi ja nõukogu määruse eelnõu üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, lk 1. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf, 01.04.2012.

⁵ Andmekaitse Inspeksioon. Isikuandmete töötlemine töösuhetes. Abistav juhendmaterjal. Tallinn: 2010. Kinnitatud 24.01.2011. Arvutivõrgus: <http://www.aki.ee/download/1818/Isikuandmed%20töösuhetes%20juhendmaterjal%20LÕPLIK.pdf>, 09.01.2012.

selline soovituslik juhised on piisav reguleerimaks töötajate jälgimist ja kontrollimist töösuhetes ning kas see kaitseb töötajat liigse privaatsusse sekkumise eest, samas tagades ka tööandja majanduslike huvide kaitse.

Töötaja privaatsuse piirangute eesmärgiks on eelkõige tööandja majanduslike huvide kaitse, näiteks jälgib tööandja sel viisil, kas töötaja kasutab oma tööaega efektiivselt ja kontrollib töötaja lojaalsust. Käesolevas töös püütakse välja pakkuda võimalikke lahendusi töötaja kontrollimiseks, mis täidaksid samu eesmärke, kuid mis sekkuksid vähem töötaja privaatsusesse.

Leidmaks vastuseid püstitatud küsimustele, on käesolevas töös kasutatud eelkõige analüüsivat ja võrdlevat meetodit. Analüüsitud on teemakohast juriidilist kirjandust, õigusakte, kohtupraktikat ning AKI juhendmaterjalid toodud juhiseid tööandjatele töötajate kontrollimiseks ja jälgimiseks. Kuna Eestis kohtupraktika sellel teemal pole veel välja kujunenud, keskendutakse antud töös kohtupraktika osas eelkõige Euroopa Inimõiguste Kohtu (edaspidi EIK) praktikale. Kuivõrd riigiti on töötaja privaatsuse piiramine töösuhetes reguleeritud erinevalt ja puudub üheselt kindel seisukoht, siis saamaks teemast paremat ülevaadet, on võrdluseks toodud näiteid ka teiste riikide – Suurbritannia ja Soome, vastavatest õigusaktidest ja seda teemat puudutavast väljakujunenud praktikast. Suurbritannia osutus valituks seetõttu, kuna seal on sarnaselt Eestiga *Information Commissioner's Office* poolt välja antud soovituslik juhised⁶ (edaspidi UK juhised) andmekaitse seaduse rakendamiseks töösuhetes. Soomes on need küsimused reguleeritud aga seaduste tasemel – privaatsuse kaitset töösuhetes⁷ ja elektroonilises sides⁸ käsitlevate seadustega.

Käesolev magistr töö koosneb kolmest peatükist, milles antakse ülevaade privaatsuse ja privaatsusõiguse olemusest, töösuhetes isikuandmete töötlemise alustest ja üldpõhimõtetest ning töötaja privaatsuse võimalikust piiramisest töösuhetes läbi töötaja kontrollimise ja jälgimise näite.

Töö esimeses peatükis määratletakse privaatsuse ja privaatsusõiguse mõiste ning kaitseala. Sellega seoses käsitletakse töötaja privaatsusega seotud põhiõigusi: õigust eraelu

⁶ Information Commissioner's Office. The Employment Practices Code, 2011. Arvutivõrgus: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/employment.aspx, 23.01.2012

⁷ Act on the Protection of Privacy in Working Life. Arvutivõrgus: <http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf>, 22.02.2012.

⁸ Act on the Protection of Privacy in Electronic Communications. Arvutivõrgus: <http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf>, 22.02.2012.

puutumatusle, õigust sõnumisaladusele, õigust vabale eneseteostusele ning õigust väljendusvabadusele. Samuti analüüsitakse, kas ja millistel tingimustel on nende põhiõiguste riive õigustatud. Lisaks käsitletakse selles peatükis ka tööandja põhiõigusi, mis töösuhetes vastanduvad töötaja põhiõigustele, kuna need tööandja põhiõigused on aluseks, et tööandjal on teatud juhtudel õigus enda põhiõiguste kaitseks töötaja privaatsusesse sekkuda.

Teises peatükis keskendutakse andmekaitse reeglitele ja põhimõtetele, kuna andmekaitse on väga oluline roll privaatsusõiguse realiseerimisel. Selles peatükis avatakse isikuandmete töötlemise põhimõisted ning tuuakse välja isikuandmete töötlemise üldised põhimõtted ja isikuandmete töötlemise õiguslikud alused. Kuna tööandja poolt töötajate kontrollimisel ja jälgimisel töödeldakse isikuandmeid, siis peab tööandja järgima neid reegleid ka töötajate kontrollimisel ja jälgimisel. Lisaks käsitletakse selles peatükis tööandja vastutust isikuandmete töötlemisel ehk millised sanktsioonid võib isikuandmete töötlemise reeglite rikkumine tööandjale kaasa tuua.

Töö kolmandas peatükis käsitletakse töötaja privaatsuse piiramist tööandja poolt läbi töötaja kontrollimise, kommunikatsioonivahendite kasutamise jälgimise ning jälgimisseadmete kasutamise. Analüüsitakse tööandja õigusi ja võimalusi töötaja kontrollimisel. Muuhulgas püütakse leida vastus küsimusele, kas ja millises ulatuses on töötajal õigus kasutada tööandja poolt tööalaseks kasutamiseks antud kommunikatsioonivahendeid isiklikuks otstarbeks. Peatükis tuuakse välja asjaolud, millistel juhtudel ja tingimustel on tööandjal õigus töötajate sidevahendite kasutust jälgida. Samuti käsitletakse jälgimisseadmete kasutamist, millistel juhtudel on selline jälgimine õigustatud ja lubatud, millised tingimused peavad olema selleks igal konkreetsel juhul täidetud ning millises ulatuses seda tööandja teha võib.

Käesoleva magistritöö hüpoteesiks on väide, et töötaja privaatsusõiguse piiramist töösuhetes puudutav õiguslik regulatsioon ei taga töötaja ega tööandja põhiseaduses sätestatud õiguste kaitset.

1. TÖÖTAJA ÕIGUS PRIVAATSUSELE

1.1 Privaatsuse ja privaatsusõiguse määratlemine

Saamaks vastust küsimusele, millises ulatuses on töötajal õigustatud ootus privaatsusele töösuhetes ja töökohal, tuleb esmalt avada privaatsuse mõiste ning määratleda privaatsusõiguse kaitseala.

Privaatsust on väga raske üheselt ja ammendavalt defineerida. Privaatsust on määratletud kui isiku eraelulist sfääri, milles on isikul õigus otsustada, kas ja kui palju ta oma eraelu teiste inimeste, avalikkuse ja riigiga jagab.⁹ Privaatsust on seostatud ka saladustega. See kaitseb võimalust hoida olulised detailid oma elust saladuses. Veel olulisem kui salajasus on aga see, et privaatsus on seotud autonoomiaga. See kaitseb võimalust valida, milliseid detaile oma elust teistele avaldada.¹⁰ Privaatsust on defineeritud ka kui ruumilist ja intellektuaalset sfääri, mis võimaldab indiviididel otsustada neid puudutavate asjaolude üle, kontrollida seda, kellel on ligipääs neid puudutavale informatsioonile ning luua ja arendada erinevaid suhteid.¹¹ Eraelu ehk privaatsus on igaühe õigus enesemääratlemisele ning õigus elada oma soovide ja tahtmiste kohaselt minimaalse välise sekkumisega.¹²

Eraelu tuleb mõista laialt, lisaks inimese intiim- ja sisemisele sfäärile laieneb kaitse ka suhetele teiste isikutega, samuti ärilistele ja sotsiaalsetele kontaktidele.¹³ Eraelu olemuse paremaks mõistmiseks võib välja tuua järgmised privaatsuse komponendid, millest eraelu koosneb:

- Identiteet

Identiteet on isiku enesemääratlus iseenda ja välismaailma jaoks ehk teisisõnu vabadus otsustada ja olla see, kes tahetakse.¹⁴ Identiteet on unikaalsete tunnuste kogum, mille alusel isik eristub kõikidest teistest isikutest. Identiteet omakorda koosneb komponentidest, mille järgi on isikut võimalik tuvastada või mille järgi isik ise ennast määratleb. Isiku identiteet hõlmab isiku nime, mõnel juhul tema identifitseerimiseks riigi poolt antud tunnusnumbrit,

⁹ M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 18.

¹⁰ S. L. Willborn. Consenting Employees: Workplace Privacy and the Role of Consent. – Louisiana Law Review 2006/66, lk 975.

¹¹ E. Palm. Privacy Expectation at Work – What is Reasonable and Why? – Ethic Theory Moral Practice 2009/12, No 2, lk 210.

¹² R. Maruste. Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn: Juura 2004, lk 429.

¹³ I. Pilving. Õigus isikuandmete kaitsele. – Juridica 2005/7, lk 533.

¹⁴ R. Maruste, lk 429.

etnilist kuuluvust, isiku välimust ja muid füüsilisi omadusi, iseloomu ja käitumist, isiku tundeid ja mõtteid, tema minevikku, usutunnistust ja muid veendumusi, tema isiklikku ruumi, sotsiaalsed võrgustikku, aga ka muid võimalikke personaalseid tunnuseid.¹⁵

- Omaette olemise ruum

Omaette olemise ruum ehk personaalne ruum on väli, milles isik saab olla privaatset, omaette, ilma välise sekkumiseta ning teadmise, et ta on omaette, segamatult.¹⁶ Üldjuhul eeldatakse, et eraelu toimub eraviisiliselt ning seetõttu peamiselt kodus, kuid see väide on ainult osaliselt õige, kuna isikul võib olla õiguspärane ootus privaatsusele ka paljudes muudes kohtades. EIK on korduvalt jõudnud järeldusele, et eraelu kaitse väljub traditsiooniliselt mõistetava elukoha raamidest, mis tähendab seda, et isikul on õigus nõuda oma privaatsuse kaitset ka väljaspool oma elukohta, näiteks töökohas või ka avalikus kohas.¹⁷

Kaasuses *Niemietz vs Saksamaa* leidis EIK, et eraelu ei pea tingimata olema seotud ainult koduga ning et õigustamatu töökoha läbiotsimine on samuti Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni¹⁸ (edaspidi EIÕK) artikliga 8 tagatud privaatsusõiguse rikkumine. Selles lahendis märgitakse, et austus eraelu vastu peab muuhulgas hõlmama ka õigust luua ja arendada suhteid teiste inimestega. Ei ole mingit põhjust, miks eraelu mõiste alt peaks välja jätma tööalase tegevuse, kuna enamiku inimeste jaoks pakub just tööelu märkimisväärset, kui mitte suurimat, võimalust arendada suhteid välismaailmaga. Seda toetab asjaolu, et alati ei ole võimalik selgelt eristada, millised inimese tegevused kuuluvad tööellu ja millised mitte.¹⁹ Euroopa andmekaitseasutuste töörühm on märkinud, et töötajad ei jäta igal hommikul tööle tulles oma õigust privaatsusele ja andmekaitsele töökoha ukse taha. Töötajatel on õiguspärane ootus privaatsusele ka töökohas, sest märkimisväärne osa suhetest teiste inimestega seondub inimese töökeskkonnaga.²⁰ Seega on töötajal õigus privaatsusele ka oma töökohal ja tööandja peab sellega arvestama.

¹⁵ M. Männiko, lk 18; E.-J. Truuväli jt (toim). Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. Tallinn: Juura 2008, § 26 komm 9.2.

¹⁶ R. Maruste, lk 433.

¹⁷ M. Männiko, lk 20.

¹⁸ Inimõiguste ja põhivabaduste kaitse konventsioon. 04.11.1950. – RT II 2010, 14, 54.

¹⁹ EIKo 16.12.1992, 13710/88, *Niemietz vs. Saksamaa*.

²⁰ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, 2002, lk 4. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf, 03.02.2012.

- Sotsiaalne suhtlemine

Lisaks identiteedile ja privaatsele ruumile moodustab osa isiku eraelust ka õigus segamatult valida suhtlusringi eri suhtlusviiside realiseerimiseks. Isikute vaheline suhtlus hõlmab isikute õigust pereelule, õigust valida sotsiaalseid kontakte ja seksuaalset orientatsiooni.²¹

- Kehaline enesemääratlusõigus

Kehaline enesemääratlus on osa isiku vabadusest, mis seisneb isiku õiguses ise otsustada oma kehalise puutumatuse üle.²²

- Keskkonnakaitse

Eraelu all ei mõisteta mitte üksnes personaalse ruumi puutumatust, vaid ka isiku õigust nõuda puhta ja segamatu elukeskkonna loomist ja säilitamist riigi poolt.²³

Isiku õigustatud ootus privaatsusele tekib läbi kahe tasandi. Esiteks peab isikul olema subjektiivne ootus privaatsusele teatud olukorras ja teiseks peab ühiskond olema valmis tunnustama seda ootust kui mõistliku ja õigustatud ootust.²⁴

Õigus privaatsusele ehk privaatsusõigus on õigus isiklikule elule, mis ühe põhiõigusena on sätestatud nii rahvusvahelistest õigusallikatest kui ka riikide konstitutsioonides. See on õigus ise määratleda, millal, kuidas ja millises ulatuses eraelulist informatsiooni teistega jagada.²⁵ Tänapäevase privaatsusõiguse ideest saab juriidilises kontekstis rääkida alates 19. sajandist. Sellest ajast pärineb kahe Ameerika õigusrevolutsionääri esimene põhjalikum käsitlus privaatsusõigusest. Juristid S. D. Warren ja L. D. Brandeis leidsid oma essee²⁶, et trükikunsti areng ja ajakirjandus tekitasid vajaduse tuletada isiku õiguse privaatsusele autoriõiguste kontseptsioonist. Pidades silmas eeskätt privaatsfääri tungivaid arenguid ajakirjanduse vallas, väitsid nad, et seaduste toel on võimalik kaitsta isiku õigust omaette olla – *right to be let alone*. Õigus privaatsusele põhines nende arusaama kohaselt isiksuse terviklikkuse põhimõttel ning tulenes üldisemast isiksusõigusest. Seda enam kui sajanditagust käsitlust privaatsusest kui isiku iseendaga seonduvast kontrolliõigusest on peetud selle tänapäeval üldtunnustatud

²¹ M. Männiko, lk 23.

²² M. Männiko, lk 30.

²³ M. Männiko, lk 33.

²⁴ S. Nouwt, B. R. De Vries, C. Prins. Reasonable Expectations of Privacy? The Hague: T.M.C. Asser Press 2005, lk 3

²⁵ S. Nouwt, B. R. De Vries, C. Prins, lk 1.

²⁶ S. D. Warren, L. D. Brandeis. The Right to Privacy. – Harvard Law Review 1890/5.

põhiõiguse süstemaatilise kaitse nurgakiviks: fraasi *right to be let alone* kasutatakse sageli privaatsusõiguse põhiolemuse selgitamiseks.²⁷

Privaatsusõigus on õigus olla jäetud rahule ja elada oma elu minimaalse välise sekkumisega. See tähendab indiviidi õigust olla isiklikus elus kaitstud:

- era- ja perekonnaelu ning kodu puutumatuse sekkumise eest;
- füüsilisse või vaimsesse puutumatusse, moraalsesse ja intellektuaalsesse vabadusse sekkumise eest;
- rünnakute eest isiku au ja vääriskuse vastu;
- isiku kohta eksitava teabe avaldamise eest;
- eraeluliste ebaoluliste ja piinlikust tekitavate faktide avaldamise eest;
- oma nime, identiteedi või isikusarnasuse kasutamise eest;
- varjatud jälgimise ja ahistamise eest;
- isiklikku kirjavahetusse sekkumise eest;
- kutsetegevuses teatavaks saanud isikut puudutavate andmete avaldamise eest;
- nii suulise kui kirjaliku isikliku suhtlemise kuritarvitamise eest.²⁸

Käesoleval ajal on Euroopa andmekaitse ja privaatsusõiguse üks olulisemaid alustalasid Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8, mis sätestab, et igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust. Ametivõimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.

Lisaks sätestab isiku õiguse privaatsusele ka ÜRO inimõiguste ülddeklaratsiooni²⁹ artikkel 12, mille kohaselt ei või kellegi isiklikku ja perekonnaellu meelevaldselt vahele segada, kellegi korteripuutumatust, kirjavahetuse saladust või au ja reputatsiooni ei tohi meelevaldselt määrada. Igal inimesel on õigus seaduse kaitsele selliste vahelesegamiste ja rikkumiste eest.

²⁷ E. Tikk, A. Nõmper. Informatsioon ja õigus. Tallinn: Juura 2007, lk 73.

²⁸ J. Michael. Privacy and human rights: an international and comparative study, with special reference to developments in information technology. Paris: UNESCO Publishing 1994, lk 13–14.

²⁹ ÜRO inimõiguste ülddeklaratsioon. 10.12.1948. Arvutivõrgus: <http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=est>, 12.03.2012.

Euroopa Liidu põhiõiguste harta³⁰ artiklis 7 sätestatakse samuti, et igal on õigus sellele, et austatakse tema era- ja perekonnaelu, kodu ja edastavate sõnumite saladust.

Seega on privaatsusõigus lühidalt öeldes õigus isiklikule elule ja selle kaitsele, see on õigus ise otsustada, kellega ja millist eraelulist informatsiooni jagada. Privaatsusõigus on rahvusvaheliselt tunnustatud põhiõigus, mille kaitseala ei piirdu kaugeltki mitte ainult isiku koduga, vaid selle põhiõiguse tulemusena on isikul õigustatud ootuse privaatsusele ka väljaspool kodu, sealhulgas töökohal. Lisaks rahvusvahelistele õigusaktidele on õigus privaatsusele tagatud ka Eesti põhiseaduses³¹ (edaspidi PS) sätestatud põhiõigustega. Järgnevalt leiavadki käsitlemist PS-s sätestatud põhiõigused, mis otseselt või kaudselt tagavad isiku õiguse privaatsusele ning milledega peab ka tööandja töösuhtes töötajat kontrollides ja jälgides arvestama.

1.1.1 Õigus vabale eneseteostusele

PS § 19 lg 1 sätestab igaühe õiguse vabale eneseteostusele. Õigus vabale eneseteostusele on isiksuse arengu, tema enesemääratlemise ning inimväärikuse väljakujunemise eelduseks ja tingimuseks. See on vabadus ise otsustada, mida teha või mida tegemata jätta ning kuidas oma elu kujundada ja ennast teostada.³²

Sellest sättest tuleneb nii üldine vabadusõigus kui ka üldine isiksusõigus.³³ Üldine isiksusõiguse esemeline kaitseala võib jagada kaheks peamiseks valdkonnaks. Esiteks hõlmab üldine isiksusõigus enesemääramisõiguse. See puudutab eelkõige isikupärimist, seksuaalseid eelistusi, sugu, soo jätkamist ja nime, samuti isiku informatsioonilist enesemääramist. Informatsiooniline enesemääratlemine tähendab igaühe õigust ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse.³⁴ Informatsioonilist enesemääramise õigust on käsitletud ka kui eraelu puutumatuse osa.³⁵

Õigus informatsioonilisele enesemääramisele on moodsa andmetöötluse tingimustes eriti tähtis. Isegi suhteliselt tähtsusetute andmete põhjal võib elektroonilise andmetöötluse abil väga hõlpsasti ja kiiresti hankida isiku kohta üksikasjalikku teavet. Loomulikult ei ole ka

³⁰ Euroopa Liidu põhiõiguste harta. – ELT eestikeelne väljaanne C 83, 30.03.2010, lk 389–403.

³¹ Eesti Vabariigi põhiseadus. – RT 1992, 26, 349 ... RT I, 27.04.2011, 2.

³² R. Maruste, lk 347.

³³ Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, § 19 komm 1.

³⁴ Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, § 19 komm 3.1.2.1.

³⁵ E. Tikk, A. Nõmper, lk 47.

õigus informatsioonilisele enesemääramisele kui osa üldisest isikuõigusest piiramatult tagatud. Andmete hädavajalik kogumine ei ole välistatud, kui see on proportsionaalne. Samas tuleb aga kaitsta isikut nende ohtude eest, mille toovad endaga isiksuse vaba eneseteostuse põlise idee realiseerimisel kaasa uued elektroonilised teabesüsteemid.³⁶

Informatsioonilisel enesemääramise õigusel on tähtis roll privaatsuse kaitsmisel. Kui isik ei saa enam ise otsustada, millises ulatuses ta end välismaailmale avalikustab, siis kaotab privaatsus oma põhiväärtuse – võimaluse enda eest vabalt otsustada.³⁷ Kui isikul ei ole võimalik piisava kindlusega teada, millist informatsiooni teda ümbritsevad inimesed tema kohta omavad, ning ta ei oska ette näha, kellele seda informatsiooni veel võidakse edastada, on olulisel määral piiratud tema vabadus oma tegevust planeerida, ilma et teda mõjutataks või talle survet avaldataks. Õigus informatsioonilisele enesemääramisele peaks välistama olukorra, kus kodanik enam ei tea, kes ja mida tema kohta teab. Kui inimene ei ole kindel, et tema käitumist ei jälgita, siis püüab ta endale võimalikult vähe tähelepanu tõmmata. Selline olukord mitte ainult ei kahjusta inimese vaba eneseteostust ja võimalusi arenguks, vaid kahjustab ka üldist heaolu, kuna kodanike vaba eneseteostus on aluseks demokraatlikule ühiskonnale.³⁸

Teiseks hõlmab üldine isiksusõigus enesekujutamise õiguse. Enesekujutamise õiguse all tuleb mõista eelkõige õigust oma kujutisele ja sõnale. Siia kuulub ka õigus otsustada ise enda kohta käivate andmete avaldamise üle. Isikul peab olema õigus ise otsustada, kas ja millisel viisil ta tahab end avalikkuse ees kujutada ning kas ja mil määral tohivad kolmandad isikud muuta tema isiksuse avaliku arutelu esemeks. Oma kujutise õigus hõlmab nii kujutise pildis kui ka liikuvus pildis. Õigus sõnale hõlmab nii igat liiki salvestused kui ka kirjalikus vormis edasi antava sõna.³⁹

1.1.2 Õigus eraelu puutumatusele

PS § 26 sätestab igäihe õiguse perekonna- ja eraelu puutumatusele. PS-ga kehtestatud eraelu puutumatuse kaitseala hõlmab kõiki eraelu valdkondi, mis ei ole kaitstud eriõigustega. Kui mõni eraeluga seotud valdkond ei ole kaetud PS §-i 26 kaitsealaga, siis kuulub see PS § 19 lg 1 kaitsealasse. Senine õiguspraktika ei võimalda siiski anda täpseid juhiseid PS § 19 lg 1 ja §

³⁶ R. Alexy. Põhiõigused Eesti põhiseaduses. – Juridica eriväljaanne 2001.

³⁷ J. C. Buitelaar, Privacy: Back to the Roots. – German Law Journal 2012/13, No 3, lk 188.

³⁸ J. Michael, lk 4.

³⁹ Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, § 19 komm 3.1.2.2.

26 kaitseala piiritlemiseks. PS § 26 kaitsealasse kuuluvad eelkõige füüsiline ja vaimne puutumatuse, isiku identiteet, isikuandmed, seksuaalsus ning õigus oma kujutisele ja sõnale.⁴⁰

PS §-s 26 sätestatud eraelu puutumatuse kaitsealas on ka juba adressaadi kontrolli alla jõudnud sõnumid ning andmed sõnumi saatmise kohta ehk nn liiklusandmed. Liiklusandmeteks on andmed sõnumi edastamise fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja isikuandmete ja asukoha kohta.⁴¹

Töösuhetes tuleb antud põhiõigusega arvestada töötaja isikuandmeid töödeldes, sest igasugune isikuandmete kogumine, salvestamine, säilitamine, avalikustamine ja muud toimingud nii riigi kui ka eraisikute poolt ohustavad isiku põhiõigusi ja sealhulgas riivavad eraelu puutumatust.⁴² Samuti peab tööandja õigusega eraelu puutumatusele arvestama töötajat kontrollides, sest töötaja füüsilist ja vaimset puutumatust võib riivata töötaja läbiotsimine või tema jälgimine.

Õigus oma kujutisele kaitseb üksikisikut tema näitamise vastu meedias ning õigus sõnale tagab seda, et isikule ei omistataks avaldusi, mida ta pole teinud.⁴³ Neid töötaja õigusi peab tööandja silmas pidama näiteks siis, kui soovib avaldada töötaja fotot ja andmeid tööandja kodulehel. Tööandja saab töötaja kohta käivaid andmeid ja fotosid oma veebileheküljele panna üksnes töötaja nõusolekul. Ka isegi juhul kui töötaja on varem andnud nõusoleku tema foto ülespanekuks ettevõtte koduleheküljel, võib töötaja IKS-i kohaselt igal ajal oma nõusoleku tagasi võtta ning tööandja on kohustatud töötaja foto ettevõtte koduleheküljelt kõrvaldama.⁴⁴

1.1.3 Õigus sõnumisaladusele

PS § 43 alusel on igal isikul õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Eesti PS-s on õigus sõnumisaladusele sätestatud eraldiseisva põhiõigusena. EIÕK artiklis 8 on õigus sõnumi saladusele sätestatud koos õigusega austusele era- ja perekonnaelu ning kodu vastu. Seega moodustab sõnumisaladus sisuliselt ühe osa eraelust.

⁴⁰ Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, § 26 komm 9.

⁴¹ Andmekaitse Inspeksioon, lk 9.

⁴² Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 26 komm 9.3.

⁴³ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 26 komm 9.5.

⁴⁴ Töösuhete käsiraamat. Tallinn: Äripäeva Kirjastus 2011, p 3.3.3.

Kuna EIÕK käsitleb õigust sõnumite puutumatusel ühes sättes koos era- ja perekonnaelu ning kodu puutumatusel ja nende kõigi õiguste piiramise alused on ühesugused (riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks), siis seetõttu ei ole EIK praktikas ka nii täpselt piiritletud, mis on sõnumisaladuse kaitseala ja mis eraelu kaitseala.⁴⁵

Eesti PS-s on need põhiõigused sätestatud eraldi paragrahvides ja seega tuleb sõnumisaladuse ja eraelu puutumatusel kaitseala piiritlemisel olla tähelepanelik, kuna PS sätestab erinevad tingimused sõnumisaladuse ja eraelu puutumatusel riivamiseks. Sõnumisaladust on lubatud riivata piiratud juhtudel – ainult kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks, samas kui eraelu puutumatusel võidakse seadusega piirata lisaks ka tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks.⁴⁶

Sõnumi saladuse kaitseala hõlmab sõnumite vahetamise posti teel ja mitmesuguste tehniliste vahendite abil. Sõnum sisaldab teavet isiku mõtete, veendumuste, arvamuste, kavatsuste, sündmuste kirjelduste ja muu kohta, mida isik sageli soovib jagada vaid valitud suhtluskaaslasel.⁴⁷ PS tagab õiguse sõnumite saladusele, mida edastatakse üldkasutataval teel. Üldkasutatavaks on sideteenus, mida sideettevõtte pakub sideteenuse turul üldistel alustel kõigile isikutele. Sõnumite saladuse kaitse tõhususe eesmärgil peaks kaitseala hõlmama kõiki edastamise viise ja vahendeid.⁴⁸ Määrav ei ole kommunikatsiooni tehniline vorm või viis, vaid teabevahetuse privaatsus.⁴⁹

Sõnumisaladus tähendab seda, et sõnumi sisu on mõeldud ainult neile, kes sõnumi saatmises ja vastuvõtmises osalevad.⁵⁰ Sõnumisaladuse kaitsealas on sõnumi sisu (mille moodustavad sõnad, märgid ja ka helid). Sõnumi saatja ei pea olema identifitseeritav. Samuti ei pea sõnumi saatja ja saaja olema erinevad isikud. Sõnumi sisu ei pea olema saladus, see võib sisult olla ka avalikkusele teada olev informatsioon. Sõnumi sisu on sõnumisaladuse kaitsealas piiratud aja jooksul – seni, kuni see on jõudnud adressaadi mõjussfääri. Kui sõnum on adressaadini juba jõudnud, on inimesel võimalik enda huvide kaitseks meetmeid kasutusele võtta. Kuid ajal, kui suhtluse osapooltel puudub kontroll sõnumi üle, peab samuti olema tagatud konfidentsiaalsus.

⁴⁵ Andmekaitse Inspeksioon, lk 8.

⁴⁶ Andmekaitse Inspeksioon, lk 7.

⁴⁷ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 43 komm 2.

⁴⁸ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 43 komm 3.

⁴⁹ R. Maruste, lk 532.

⁵⁰ R. Maruste, lk 532.

PS § 43 eesmärk ongi luua vajalikud garantiid selleks, et sõnum saaks konfidentsiaalselt adresseeritud toimetatud. Pärast seda, kui sõnum on adresseeritud kontrolli alla jõudnud, kohalduvad sellele PS § 26 sätestatud üldine eraelu kaitse.⁵¹

Sõnumis sisalduva teabega on seotud juba eelnevalt mainitud nn liiklusandmed – andmed elektroonilise side võrgu kaudu edastatavate sõnumite edastamise fakti, kestuse, viisi ja vormi ning andmete edastaja ja vastuvõtja isikuandmete ja asukoha kohta. Nendest andmetest ei selgu sõnumi sisu, mistõttu taoliste andmete kogumine kuulub eraelu kaitsealasse.⁵²

EIK praktika kohaselt, kuulub EIÕK artikkel 8 kaitsealasse sõnumite edastamine ja vastuvõtmine nii eravaldu, äriühingus kui ka ametiasutuses. EIK on seisukohal, et eraelu puutumatuse ja sõnumisaladuse kaitseala laieneb ka töötaja töötelefonilt tehtud kõnedele ning töötaja e-kirjadele ja internetikasutusele.⁵³ Seega hõlmab sõnumite saladuse kaitse ka töötaja poolt töökohal edastatavaid või vastuvõetavaid sõnumeid (kirjad, e-kirjad, telefonikõned, lühisõnumid, msn-i vestlused, faksid jm sõnumid) vaatamata sellele, et sõnumi saatmiseks või vastuvõtmiseks kasutatavad tehnilised vahendid võivad kuuluda tööandjale ja vastava sideteenuse osutamine toimub tööandja kulul.

Vastavalt PS § 9 lg-le 2, mis sätestab, et põhiseaduses loetletud õigused, vabadused ja kohustused laienevad juriidilistele isikutele niivõrd, kui see on kooskõlas juriidiliste isikute üldiste eesmärkide ja selliste õiguste, vabaduste ja kohustuste olemusega, laieneb sõnumisaladuse kaitse ka juriidilistele isikutele, mistõttu on sõnumisaladusega kaitstud ka tööandja kirjad ja telefonikõned. Samas tööandja ja töötaja vahelistes suhetes tuleb töötaja personaalsesse sõnumisaladuse kaitsealasse kuuluvaks lugeda siiski vaid töötaja erakirjad ja – telefonikõned. Tööalased kirjad ja kõned teebki töötaja tööandja nimel ja tööandja jaoks.⁵⁴

1.1.4 Õigus väljendusvabadusele

Vastavalt PS § 45 on igaühel õigus vabalt levitada ideid, arvamusi, veendumusi ja muud informatsiooni sõnas, trükis, pildis või muul viisil. Väljendusvabadus on väärtus iseenesest, olles tähtis eeldus ja tingimus ka mitme muu õiguse ja vabaduse sisuliseks ja asjakohaseks toimimiseks ja kaitseks, sealhulgas on see oluline ka informatsioonilise enesemääramise

⁵¹ Andmekaitse Inspeksioon, lk 8–9.

⁵² Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 43 komm 5.

⁵³ EIKo 25.06.1997, 20605/92, *Halford vs. Ühendkuningriik*; EIKo 09.04.2007, 62617/00, *Copland vs. Ühendkuningriik*.

⁵⁴ Andmekaitse Inspeksioon, lk 9.

õiguse ja privaatsusõiguse kasutamisel. Ilma täiemahulise väljendusvabaduseta on teiste õiguste ja vabaduste vaba toimimine piiratud.⁵⁵

Töötaja väljendusvabadust riivavad näiteks piirangute seadmine internetis kommenteerimisele ja ajaveebi pidamisele, aga ka telefonikõnede pealtkuulamine ja lindistamine ning e-kirjade lugemine.⁵⁶

1.2 Töötaja põhiõigustele vastanduvad tööandja põhiõigused

Kui töötaja privaatsuse kaitse huvides on, et tööandja koguks tema kohta võimalikult vähe isikuandmeid ning kontrolliks ja jälgiks teda samuti ainult äärmisel vajadusel, siis tööandjal on oma põhiseadusega tagatud õiguste kaitseks vastupidised huvid. Tööandja tahab omada töötajate kohta võimalikult palju informatsiooni, et olla kindel töötajate võimetes ja oskustes täita nendele töölepinguga pandud kohustusi. Selleks on näiteks tööandja huvitatud värbamisel töötaja varasematest töökogemustest, töösuhtes aga soovib tööandja kontrollida töötaja tööülesannete täitmist, nii seda, kui efektiivselt ja kvaliteetselt töötaja oma kohustusi täidab, kui ka seda, kas töötajad on talle lojaalsed ja peavad kinni konfidentsiaalsuskohustusest. Töötaja õigus privaatsusele peab olema tasakaalus tööandja õiguste ja huvidega, eelkõige tööandja õigusega juhtida edukalt oma ettevõtet ning õigusega kaitsta end vastutuse ja kahju eest, mida töötajad oma tegevusega võivad põhjustada. Need tööandja õigused ja huvid moodustavad õigusliku aluse õigustamaks asjakohaseid meetmeid töötaja privaatsusõiguse piiramiseks.⁵⁷

Seega on töösuhtes nii tööandjal kui töötajal omad huvid ja õigused, mida nad kaitsta soovivad, kuid nende õiguste kasutamise ja huvide kaitsmisel peavad töösuhte mõlemad pooled arvestama PS § 19 lg-ga 2, mis sätestab, et igaüks peab oma õiguste ja vabaduste kasutamisel ning kohustuste täitmisel austama ja arvestama teiste inimeste õigusi ja vabadusi ning järgima seadust.

Järgnevalt leiavad käsitlemist tööandja põhiõigused, mis töösuhtes teatud juhtudel vastanduvad eespool käsitletud töötaja põhiõigustele ning millede teostamisel peab tööandja

⁵⁵ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 45 komm 4.

⁵⁶ Andmekaitse Inspeksioon, lk 9.

⁵⁷ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 4.

arvestama töötaja põhiõigustega. Kuid samas annavad need põhiõigused ka aluse selleks, et tööandja võib teatud juhtudel oma õiguste ja huvide kaitseks töötaja privaatsust piirata.

1.2.1 Ettevõtlusvabadus

PS § 31 alusel on Eesti kodanikel õigus tegeleda ettevõtlusega ning koonduda tulundusühingutesse ja -liitudesse. Selle paragrahviiga sätestatakse õigus tegeleda ettevõtlusega ehk ettevõtlusvabadus, mis laieneb ka juriidilistele isikutele.

Ettevõtlus on tegevus, mille eesmärgiks üldjuhul on tulu saamine kauba tootmisest, müümisest, teenuste osutamisest, vara realiseerimisest jne. Ettevõtlusvabaduse esemeline kaitseala hõlmab kõiki tegevusalasid ja elukutseid, mille puhul isik pakub enda nimel kaupu või teenuseid. Ettevõtlusvabadust riivab iga abinõu, mis takistab, kahjustab või kõrvaldab mõne ettevõtlusega seotud tegevuse.⁵⁸

Arvestades, et ettevõtjad kasutavad oma tegevuses sageli teiste isikute, s.o töötajate abi, siis on selge, et ettevõtlusega tegelejal, kes on ühtlasi ka tööandja, on vaja teatavat kontrolliõigust oma töötajate suhtes ning võimalust koguda nende kohta mitmesugust ettevõtluse toimimise tagamiseks vajalikku informatsiooni. Vastasel juhul puuduks ettevõtjal ülevaade oma tegevusest ning võimalus seda suunata, mistõttu ei saaks ettevõtja oma tegevuse eest vastutada. Seega tulebki ettevõtlusvabaduse kaitse alla arvata ettevõtja õigus koguda ja saada mitmesugust ettevõtluse toimimiseks vajalikku teavet, sealhulgas oma töötajate kohta.⁵⁹

1.2.2 Omandipõhiõigus

Vastavalt PS §-le 32 on igapäevane omand puutumatu ja võrdselt kaitstud ning igapäevane on õigus enda omandit vabalt vallata, kasutada ja käsutada. Seadusega võidakse sätestada kitsendusi omandiõiguse teostamisel.

Kuivõrd töösuhted on alati seotud suuremal või vähemal määral tööandja varaga (töövahendid, tooraine, toodang, intellektuaalne omand), on tööandjal huvi kaitsta oma omandiõigust. Tööandja omandiõigust rikuvad nii vara kahjustamine kui kaotsimine.⁶⁰ Tööandja omandiõigust võib kahjustada ka töötaja konfidentsiaalsuskohustuse rikkumine ja

⁵⁸ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 41 komm 5, 8.

⁵⁹ A. Henberg. Isikuandmete töötlemine töösuhetes. – Juridica 2005/8, lk 560.

⁶⁰ Andmekaitse Inspektsioon, lk 10.

ärisaladuse avaldamine, eelkõige ohustab selline töötajapoolne kohustuste rikkumine tööandja intellektuaalset omandit.

Kui Eestis peab tööandja oma omandipõhiõiguse teostamisel arvestama töötaja põhiõigustega, siis näiteks Ameerika Ühendriikides on levinud arusaam, mille kohaselt töötajale tööülesannete täitmiseks eraldatud töövahendid on tööandja omand ja sellest tulenevalt on tööandjal ka täielik võim oma vara kasutamise üle. Kuna töövahendid kuuluvad tööandjale, siis puudub seal ka töötajal õigus privaatsusele töökohal.⁶¹

1.3 Privaatsusõiguse kui põhiõiguse riive lubatavus ja proportsionaalsus

Õigus privaatsusele ei ole oma loomult absoluutne õigus, mis tähendab seda, et õigusliku aluse olemasolul on riive lubatud.⁶² Põhiõiguse riive mõistet tuleb hoida rangelt lahus põhiõiguse rikkumise mõistest. Põhiõiguse riive on põhiõiguse rikkumine ainult siis, kui see on formaalselt või materiaalselt põhiseadusevastane.⁶³ PS sätestab konkreetsed tingimused, millistel juhtudel võib põhiõigusi piirata. PS § 11 alusel tohib õigusi ja vabadusi piirata ainult kooskõlas põhiseadusega. Need piirangud peavad olema demokraatlikus ühiskonnas vajalikud ega tohi moonutada piiratavate õiguste ja vabaduste olemust. Põhiõiguse iga riive peab vastama kõigile põhiseaduse normidele. PS-ga kooskõla tingimused sõltuvad sellest, mis liiki põhiõigusega on tegu.⁶⁴

Alus PS § 19 lg-s 1 sätestatud õiguse vabale eneseteostusele ehk üldise vabaduspõhiõiguse piiramiseks tuleneb PS § 19 lg-st 2, mis kehtestab põhikohustuse oma õiguste ja vabaduste kasutamisel ning kohustuste täitmisel austada ja arvestada teiste inimeste õiguste ja vabadustega ning järgida seadust. PS § 19 lg 1 on lihtsa seadusereservatsiooniga põhiõigus ja sellest lähtuvalt võib üldist vabaduspõhiõigust piirata mis tahes põhjusel, mis ei ole PS-ga otseselt keelatud. Lisaks sätestab PS § 19 lg 2 põhiõiguste kolmikmõju ehk kehtivuse eraisikute vahelistele suhetele. Kuna kellegi vabadus ei saa olla piiramata, siis sellest tulenevalt sätestavad põhiõigused lõppastmes ka eraisikute omavahelistes suhetes teatud

⁶¹ A. Jõks. Eraelu kaitse töösuhetes – väljakutse tööandjale. Ettekanne Andmekaitse inspektsiooni konverentsil, 27.01.2010. Arvutivõrgus:

[http://www.aki.ee/download/1480/allarj%20270110%20%20PPT\(1733968_1\)%20ettekanne%202%20\[Kirjutuskaitstud\].pdf](http://www.aki.ee/download/1480/allarj%20270110%20%20PPT(1733968_1)%20ettekanne%202%20[Kirjutuskaitstud].pdf), 19.02.2012.

⁶² M. Männiko, lk 34.

⁶³ R. Alexy. Põhiõigused Eesti põhiseaduses.

⁶⁴ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 11 komm 2.

õigusi ja kohustusi.⁶⁵ Seega peab töötaja oma põhiõigusi teostades arvestama tööandja põhiõigustega, nagu PS §-s 31 sätestatud ettevõtlusvabadusega ja PS §-st 32 tuleneva õigusega omandi puutumatusele.

Vastavalt PS §-le 26 võib eraellu sekkuda ainult seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Üheks seaduseks, mis sätestab piirangud PS §-le 26, on IKS. IKS-i kohaselt võib alus töötaja isikuandmete töötlemiseks (ehk põhiõiguste riiveks) tuleneda ka muust seadusest, samuti võib isikuandmeid töödelda isiku enda nõusolekul.⁶⁶

Õigust sõnumisaladusele võib piirata vastavalt PS §-s 43 sätestatule ainult kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras. Õigust sõnumisaladusele võimaldavad piirata vaid kriminaalmenetluse seadus, jälitustegevuse seadus ning julgeolekuasutuste seadus. Seega isikuandmete kaitse seaduses sätestatud alused isikuandmete töötlemiseks ei ole kohaldatavad sõnumisaladuse riive õigustamiseks ja ka üheski teises seaduses pole kehtestatud tööandjale alust töötaja sõnumisaladuse riiveks.⁶⁷

Väljendusvabaduse piiramise alus tuleneb PS § 45 teisest lausest, lubades seda õigust seadusega piirata avaliku korra, kõlbluse, teiste inimeste õiguste ja vabaduste, tervise, au ning hea nime kaitseks, ning sama paragrahvi kolmandast lausest, mis kehtestab, et seadusega võib seda õigust piirata ka riigi ja kohaliku omavalitsuste teenistujatel neile ameti tõttu teatavaks saanud riigi- ja või ärisaladuse või konfidentsiaalsena saadud informatsiooni ning teiste inimeste perekonna- ja eraelu kaitseks, samuti õigusemõistmise huvides.

Privaatsusõiguse riive õiguspärasuse alused tulenevad ka EIÕK artikli 8 lõikest 2 - ametivõimud ei sekku privaatsusõiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks. Seega peavad riive lubatavuseks esinema kaks olulist komponenti – riive peab toimuma kooskõlas seadusega ja riive peab olema vajalik demokraatlikus ühiskonnas.⁶⁸

⁶⁵ Eesti Vabariigi Põhiseadus, § 19 komm 3.4.2, 5.

⁶⁶ Andmekaitse Inspeksioon, lk 11.

⁶⁷ Andmekaitse Inspeksioon, lk 9.

⁶⁸ M. Männiko, lk 35.

Lisaks põhiõiguste riivete formaalõiguslikele alustele tuleb hinnata ka riivete proportsionaalsust. Proportsionaalsuse põhimõtte tähendab, et piiranguks olev abinõu peab olema sobiv, vajalik kitsamas tähenduses ja proportsionaalne kitsamas tähenduses ehk mõõdukas.

Sobiv on abinõu, mis soodustab eesmärgi saavutamist. Vaieldamatult ebaproportsionaalne on sobivuse mõttes abinõu, mis ühelgi juhul ei soodusta eesmärgi saavutamist. Vajalik ei ole, et abinõu eesmärgi absoluutse kindlusega saavutaks. Piisab, kui tegemist on sammuga õiges suunas, vahendiga, mis seatud eesmärgi saavutamisele kaasa aitab, seda edendab.⁶⁹

Abinõu on vajalik, kui eesmärki ei ole võimalik saavutada mõne teise, kuid isikut vähem koormava abinõuga, mis on vähemalt sama efektiivne kui esimene. Arvestada tuleb ka seda, kuivõrd koormavad erinevad abinõud kolmandaid isikuid, samuti erinevusi kulutustes.⁷⁰

Abinõu on mõõdukas, kui kasutatud vahendid on proportsionaalsed soovitud eesmärgiga. Piirangud ei tohi kahjustada kaitstud õigust rohkem, kui see on normi legitiimse eesmärgiga põhjendatav. Abinõu mõõdukuse üle otsustamiseks tuleb kaaluda ühelt poolt põhiõigusesse sekkumise ulatust ja intensiivsust, teiselt poolt aga eesmärgi tähtsust, sest mida intensiivsem on põhiõiguse riive, seda mõjuvamad peavad olema riivet õigustavad põhjused.⁷¹

Seega töötaja privaatsusõigus ei ole absoluutne ja teatud juhtudel on selle õiguse piiramine töösuhtes lubatud. Samas peab sekkumine töötaja privaatsusse olema alati põhjendatud ja mitte riivama töötaja õigust rohkem, kui see on konkreetse eesmärgi saavutamiseks vajalik. Tasakaalu leidmiseks töösuhte poolte põhiõiguste vahel ning nende õiguste ja huvide piisava kaitse tagamise eesmärgil, tuleb enne töötajate privaatsust riivavate meetmete rakendamist hoolikalt kaaluda, kas tööandja õigustatud huvi on piisav sellise piirangu rakendamiseks ning ega ei ole töötaja privaatsust vähem riivavamaid võimalusi sama eesmärgi saavutamiseks.

⁶⁹ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 11 komm 3.1.

⁷⁰ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 11 komm 3.2.

⁷¹ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 11 komm 3.3.

2. ISIKUANDMETE TÖÖTLEMINE TÖÖSUHETES

2.1 Isikuandmete töötlemise ja selle piiramise vajalikkus

Isikuandmete töötlemine töösuhetes on väga tihedalt seotud töötaja privaatsusõigusega. Kuna on selge, et isikuandmete kogumine, säilitamine, kasutamine ja avalikustamine võib kaasa tuua otseseid või kaudseid tagajärgi eraelu puutumatusele,⁷² siis eksimine isikuandmete töötlemise reeglite vastu võib põhjustada tõsise töötaja privaatsusõiguse riive ja ohustada töötaja eraelu puutumatust. EIK on oma otsuses leidnud, et pelk eraelu puudutavate andmete kogumine kujutab endast juba isiku privaatsusesse sekkumist ning kogutud isikuandmete edasisel kasutamisel ei ole siin mingisugust tähendust.⁷³ Nii tööandjad kui töötajad peaksid teadma, et paljud rutiinsed tegevused töösuhetes toovad kaasa töötajate isikuandmete töötlemise, mõnikord isegi väga delikaatsete andmete töötlemise.⁷⁴ Samas ilma isikuandmete töötlemiseta ei ole võimalik töösuhteid luua ega töösuhetes olla.

Töötajad peavad arvestama, et seni, kuni nad kuuluvad tööandja organisatsiooni, peavad nad leppima teatud määral nende privaatsusõigusesse sekkumisega ning jagama teatud isiklikku informatsiooni tööandjaga. Tööandjal on õigustatud huvi töödelda töötajate isikuandmeid seaduslikel eesmärkidel, mis on vajalikud töösuhte ja äritegevuse normaalseks arenguks.⁷⁵

Kuna info- ja kommunikatsioonitehnoloogiad võimaldavad isikuandmeid massiliselt koguda ja töödelda, kujutab seesugune tegevus ohtu üksikisiku eraelu puutumatusele ning üldisele isiksusõigusele: erinevaid andmeid kombineerides on võimalik luua võrdlemisi terviklik pilt isiku omadustest, harjumustest, suhetest, varalisest seisust jms ning seeläbi kaudselt inimest n-ö jälgida.⁷⁶ Tuginedes informatsioonile, millal, kus ja kuidas töötaja oma tööülesandeid täidab, võib tööandja saada väga detailse ettekujutuse töötaja jõudlusest ning kombineerides ja töödeldes neid andmeid teiste jälgimise käigus kogutud või muude tööandja valduses olevate töötaja isikuandmetega, võimaldab see tööandjal saada töötajast kõikehõlmava

⁷² L. Wildhaber, O. Diggelmann. Euroopa inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. – Juridica 2007/1, lk 5.

⁷³ EIKo 16.02.2000, 27798/95, *Amann vs. Šveits*.

⁷⁴ Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context, lk 2. Arvutivõrgus: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf>, 03.02.2012.

⁷⁵ Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context, lk 19.

⁷⁶ T. Ilus. Andmesubjekti osaluse põhimõtte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. – Juridica 2005/8, lk 522.

kujutise, mida tavaliselt oleks võimalik saavutada ainult lähedase isikliku suhte tulemusena.⁷⁷ Seetõttu tuleb andmetöötlust põhiseaduslike õiguste kaitseks piirata, et iga inimene saaks ise võimalikult palju otsustada, kui palju ta end teistele isikutele ning laiemale avalikkusele nähtavaks teeb.⁷⁸

Eesti põhiseaduses ei ole eraldi põhiõigusena nimetatud õigust isikuandmete kaitsele, vaid see on tuletatav põhiõiguste kaudu, mida käsitleti eelmises peatükis. Riigikohus on PS § 10 alusel leidnud, et Euroopa õigusruumis üldtunnustatud põhiõigused kehtivad ka Eestis.⁷⁹ Õigus isikuandmete kaitsele on selgelt sätestatud Euroopa Liidu põhiõiguste hartas artiklis 8 – igal inimesel on õigus oma isikuandmete kaitsele. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igal inimesel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist. Nende sätete täitmist kontrollib sõltumatu asutus. Samuti on õigus isikuandmete kaitsele sätestatud Euroopa Liidu toimimise lepingu artiklis 16.⁸⁰

Andmete kaitsmine põhiõigustega ei tähenda veel andmete töötlemise keeldu, vaid paneb riigile töötlemise reguleerimise ja selle vajalikkuse kaalumise kohustuse.⁸¹ Töötajate privaatsust ja inimväärikust, iseäranis võimalust sotsiaalseteks ja isiklikeks suheteks töökohal, tuleb kaitsta töösuhetes isikuandmete kogumisel ja kasutamisel.⁸² Seega ongi riik kehtestanud andmekaitse reeglid ja põhimõtted, millega peab arvestama ka tööandja töötaja isikuandmeid töödeldes, tagamaks töötaja privaatsuse kaitse.

Isikuandmete töötlemise piiramisele suunatud andmekaitse reeglid lähtuvad eeldusest, et isikuandmete töötlemine on vajalik. Vastasel juhul, ei oleks andmekaitse põhimõtteid vajagi, piisaks ainsast ühemõttelisest reeglist: isikuandmete töötlemine on keelatud. Andmekaitse konstruktiivne eesmärk ei saa seetõttu olla isikuandmete kasutamise võimalikult laiaulatuslik keelamine, vaid andmesubjekti huvide tõhus kaitse olukorras, kus teised isikud tema kohta käivat teavet paratamatult kasutavad.⁸³ Nagu juba eelnevalt öeldud, on isikuandmete

⁷⁷ E. Palm, lk 207.

⁷⁸ T. Ilus, lk 522.

⁷⁹ I. Pilving, lk 535.

⁸⁰ Euroopa Liidu toimimise leping. – ELT eestikeelne väljaanne C 83, 30.03.2010, lk 47–199.

⁸¹ I. Pilving, lk 536.

⁸² Council of Europe Committee of Ministers. Recommendation No. R (89) 2 on the protection of personal data used for employment purposes, p 2. Arvutivõrgus: <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276592&SecMode=1&DocId=699842&Usage=2>, 20.02.2012.

⁸³ T. Ilus, lk 519.

töötlemine töösuhtes vajalik, kuna see tuleneb töösuhte loomusest. Ilma isikuandmete töötlemiseta töösuhe lihtsalt ei toimiks.

2.2 Isikuandmete töötlemise põhimõisted

Isikuandmeteks on IKS § 4 lg 1 kohaselt mis tahes andmed tuvastatud või tuvastatava füüsilise isiku kohta, sõltumata sellest, millisel kujul või millises vormis need andmed on. Tuvastatav on isik, keda saab otseselt või kaudselt tuvastada, eelkõige isikukoodi põhjal või tema ühe või mitme füüsilisele, füsioloogilisele, vaimsele, majanduslikule, kultuurilisele või sotsiaalsele identsusele omase joone põhjal.⁸⁴ Isikuandmeteks on nii objektiivne teave, näiteks mingi aine sisaldus veres, kui ka subjektiivne teave, nagu arvamused ja hinnangud. Isikuandmete mõiste laieneb mistahes vormis teabele: see võib esineda sõnadena, numbritena, graafiliselt, fotona või helina. Teave võib esineda näiteks paberkandjal, samuti arvuti mälus kahendkoodis või näiteks videol.⁸⁵ Isikuandmeteks on näiteks isiku nimi, isikukood, e-postiaadress, aga ka häääl ja kujutis (näiteks foto, audio- või videosalvestise kujul), kui need võimaldavad isikut kas või kaudselt tuvastada.⁸⁶ Selleks, et teave kujutaks endast isikuandmeid, ei pea see olema tingimata tõene või tõendatud.⁸⁷ Ebaõige teabe korral on isikul õigus see vaidlustada ning nõuda selle parandamist.

Isikuandmete seas eristatakse delikaatseid isikuandmeid, millede töötlemise alused on piiratud ning reeglid töötlemiseks on rangemad. Delikaatsed isikuandmed vastavalt IKS § 4 lg-le 2 on:

- poliitilisi vaateid, usulisi ja maailmavaatelisi veendumusi kirjeldavad andmed, välja arvatud andmed seadusega ettenähtud korras registreeritud eraõiguslike juriidiliste isikute liikmeks olemise kohta;
- etnilist päritolu ja rassilist kuuluvust kirjeldavad andmed;
- andmed tervise seisundi või puude kohta;
- andmed pärilikkuse informatsiooni kohta;

⁸⁴ Euroopa Parlamendi ja Nõukogu 24.10.1995.a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 23.11.1995, lk 31–50 (eestikeelne eriväljaanne: ptk 13, kd 015, lk 355–374), (edaspidi andmekaitse direktiiv), artikkel 2 punkt a.

⁸⁵ Artikli 29 alusel loodud andmekaitse töörühm. Arvamus 4/2007 isikuandmete mõiste kohta, lk 6–7. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_et.pdf, 03.02.2012.

⁸⁶ Article 29 Data Protection Working Party. Working document on the Processing of Personal Data by means of Video Surveillance, 2002, lk 5. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp67_en.pdf, 03.02.2012.

⁸⁷ Artikli 29 alusel loodud andmekaitse töörühm. Arvamus 4/2007 isikuandmete mõiste kohta, lk 6.

- biomeetrilised andmed (eelkõige sõrmejälje-, peopesajälje- ja silmaiirisekujutis ning geenandmed);
- andmed seksuaalelu kohta;
- andmed ametiühingu liikmelisuse kohta;
- andmed süüteo toimepanemise või selle ohvriks langemise kohta enne avalikku kohtuistungit või õigusrikkumise asjas otsuse langetamist või asja menetluse lõpetamist.

Isikut, kelle isikuandmeid töödeldakse, nimetatakse andmesubjektiks. Isikuandmete töötlemiseks on IKS § 5 alusel iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, riskasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest.

Seega töötleb tööandja töötaja isikuandmeid ka käesoleva töö põhiliseks uurimisobjektiks oleval töötajate ja töötaja poolt kasutatavate kommunikatsioonivahendite kasutamise kontrollimisel ja jälgimisel. Vastavalt TLS § 41 lg-le 2 peab tööandja tagama töötaja isikuandmete töötlemise vastavalt isikuandmete kaitse seadusele. Järgnevates alapeatükkides käsitletaksegi, millistel alustel tööandja töötaja isikuandmeid töödelda võib ning milliseid põhimõtteid seejuures järgida tuleb.

2.3 Isikuandmete töötlemise õiguslikud alused

Isikuandmete töötlemine toimub põhiliselt kahel alusel – andmesubjekti nõusolekul (IKS § 10 lg 1) ja andmesubjekti nõusolekuta seadusest tuleneval alusel (IKS § 14 lg 1 p1). Nende aluste rakendamisest töösuhetes lähemalt järgnevates alapunktides.

Lisaks võib IKS § 14 lg 1 alusel isikuandmeid ilma isiku nõusolekuta töödelda välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud ülesande täitmiseks (p 2), üksikjuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada (p 3) ja andmesubjektiga sõlmitud lepingu täitmiseks või lepingu täitmise tagamiseks, välja arvatud delikaatsete isikuandmete töötlemine (p 4).

Andmekaitse direktiivis toodud alused isikuandmete töötlemiseks kattuvad osaliselt IKS-s sätestatud alustega. Lisaks eespool toodud alustele näeb andmekaitse direktiiv võimaluse isikuandmete töötlemiseks juhul, kui töötlemine on vajalik üldiste huvidega seotud ülesande täitmiseks või sellise avaliku võimu teostamiseks, mis on tehtud ülesandeks volitatud töötlejale või andmeid saavale kolmandale isikule (artikkel 7 punkt e) ning kui töötlemine on vajalik vastutava töötleja või andmeid saava kolmanda isiku õigustatud huvide elluviimiseks, kui selliseid huve ei kaalu üles andmesubjekti põhiõiguste ja -vabadustega seotud huvid (artikkel 7 punkt f).

Erinevalt IKS-st kehtestab andmekaitse direktiivi artikkel 8 eriregulatsiooni delikaatsete isikuandmete töötlemisele, keelates üldjuhul delikaatsete isikuandmete töötlemise, kuid sätestades erijuhud, mil delikaatsete isikuandmete töötlemine on lubatud. Sellisteks delikaatsete isikuandmete töötlemise erandlikeks alusteks, mida IKS-s ei ole sätestatud, on:

- töötlemine on vajalik seoses vastutava töötleja kohustuste ja eriõigustega tööõiguse valdkonnas, kuivõrd see on lubatud siseriikliku õigusega, milles on sätestatud piisavad tagatised (artikkel 8 punkt b);
- töötlemine toimub poliitilise, filosoofilise, religioosse või ametiühingulise suunitlusega ühenduse tegevuse raames ning töötlemine käsitleb ainult asjaomase ühenduse liikmeid või seotud isikuid ning andmeid ei avalikustata kolmandatele isikutele ilma andmesubjekti nõusolekuta (artikkel 8 punkt d);
- töötlemine on vajalik õigusnõuete koostamiseks, esitamiseks või kaitsmiseks (artikkel 8 punkt e).

2.3.1 Seadusest tulenevad alused

Isikuandmete töötlemise seadusest tulenevad alused on: IKS-s sätestatud juhud, eriseadustes sätestatud alused, mis annavad tööandajale õiguse või panevad kohustuse töödelda töötaja isikuandmeid (näiteks TLS, töötervishoiu ja tööohutuse seadus) ning välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduvast õigusaktist tulenevad alused.

Töösuhtes võivad kohaldamisele tulla järgmised IKS-s sätestatud alused, mil andmeid võib töödelda ilma andmesubjekti nõusolekuta:

- IKS § 14 lg 1 p 4 - andmesubjektiga sõlmitud lepingu täitmiseks või lepingu täitmise tagamiseks, välja arvatud delikaatsete isikuandmete töötlemine;
- IKS § 14 lg 2 p 2 - üksikjuhtumil andmesubjekti või muu isiku elu, tervise või vabaduse kaitseks, kui andmesubjektilt ei ole võimalik nõusolekut saada (kehtib isikuandmete edastamise või nendele juurdepääsu võimaldamise kohta kolmandale isikule andmete töötlemiseks);
- IKS § 14 lg 3 kohaselt isikute või vara kaitseks jälgimisseadustiku kasutamisel.⁸⁸

Peamine alus isikuandmete töötlemiseks töösuhetes on IKS § 14 lg 1 p 4 ehk siis töötleb tööandja töötaja isikuandmeid töölepingu täitmiseks või täitmise tagamiseks. Samas on mõned õiguspraktikud seisukohal, et töösuhetes toimub isikuandmete töötlemine töötaja nõusolekul, mis tuleb anda töölepingu sõlmimisel. Nimetatud seisukohaga ei saa nõustuda, kuna sellisel juhul võib tekkida olukord, kus töötaja võtab oma nõusoleku IKS § 12 lg 7 alusel tagasi ja tööandja peab isikuandmete töötlemise lõpetama. Samas ei ole praktikas mõeldav töösuhte jätkumine ilma, et tööandja töötaja isikuandmeid töötleks, kuna töötaja isikuandmete töötlemine on töösuhte igapäevane lahutamatu osa.⁸⁹

2.3.2 Töötlemine töötaja nõusolekul

Vastavalt IKS §-le 10 on isikuandmete töötlemine lubatud ainult andmesubjekti nõusolekul, kui seadus ei sätesta teisiti. IKS § 12 sätestab tingimused, millele peab nõusolek isikuandmete töötlemiseks vastama. Vastavalt kehtestatud tingimustele peab tahteavaldus tuginema isiku vabal tahtel. Selles peavad olema selgelt määratletud andmed, mille töötlemiseks luba antakse, andmete töötlemise eesmärk ning isikud, kellele andmete edastamine on lubatud, samuti andmete kolmandatele isikutele edastamise tingimused ning andmesubjekti õigused tema isikuandmete edasise töötlemise osas. Nõusolek peab olema kirjalikku taasesitamist võimaldavas vormis, välja arvatud juhul, kui vorminõude järgmine ei ole andmetöötluste erilise viisi tõttu võimalik. Kui nõusolek antakse koos teise tahteavaldusega, peab isiku nõusolek olema selgelt eristatav. Delikaatsete isikuandmete töötlemiseks antud nõusolek peab olema antud alati kirjalikku taasesitamist võimaldavas vormis.

⁸⁸ Andmekaitse Inspeksioon, lk 12.

⁸⁹ Andmekaitse Inspeksioon, lk 12.

Enne andmesubjektilt isikuandmete töötlemiseks nõusoleku küsimist peab isikuandmete töötleja andmesubjektile teatavaks tegema isikuandmete töötleja või tema esindaja nime ning isikuandmete töötleja aadressi ja muud kontaktandmed.

Andmesubjekti nõusolek kehtib andmesubjekti eluajal ning 30 aastat pärast andmesubjekti surma, kui andmesubjekt ei ole otsustanud teisiti. Nõusoleku võib andmesubjekt igal ajal tagasi võtta, kuid nõusoleku tagasivõtmisel ei ole tagasiulatuvat jõudu. Seoses sellega, et töötaja võib oma nõusoleku igal ajal tagasi võtta, saab töötaja nõusolek töösuhtes isikuandmete töötlemise aluseks olla vaid neil juhtudel, kui isikuandmete töötlemine ei ole vältimatu ning töötajal on tõepoolest võimalik otsustada, kas ta soovib anda nõusoleku isikuandmete töötlemiseks ning tal on realselt võimalus nõusolek tagasi võtta, ilma et sellega kaasneks kahju.⁹⁰

Töösuhtes töötaja nõusoleku alusel töötaja isikuandmete töötlemine on ohtlik ja seda tuleks üldjuhul vältida. Mõned andmekaitse ametnikud ei pea töötaja nõusolekut üldse kehtivaks õiguslikuks aluseks, kuna töötaja võib olla sunnitud nõusolekut andma.⁹¹ Kui töötaja annab ära osa oma õigusest privaatsusele, peab ta seda tegema üheselt mõistetava nõusoleku andmisega. Kehtiv on ainult nõusolek, mis on antud vabatahtlikult ja mille võib andmesubjekt igal ajal tagasi võtta. Paraku töösuhte puhul ei ole võimalik neid tingimusi alati järgida ja seega ei saa isikuandmete töötlemine töösuhetes üldjuhul toimuda töötaja nõusoleku alusel.

2.4 Isikuandmete töötlemise põhimõtted

Isikuandmete töötlemisel tuleb alati järgida IKS §-s 6 sätestatud isikuandmete töötlemise põhimõtteid, seda nii seaduse alusel kui ka töötaja nõusoleku alusel toimuval isikuandmete töötlemisel. Antud põhimõtete eesmärk on kaitsta isikuandmete töötlemisel andmesubjekti liigse ja mittevajaliku põhiõiguste riive eest.

- Seaduslikkuse põhimõte – isikuandmeid võib koguda vaid ausal ja seaduslikul teel. Isikuandmete töötlemisega ei tohi seadusliku aluseta piirata andmesubjektide õigust eraelu

⁹⁰ Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context, lk 23.

⁹¹ C. Kuner. European Data Protection Law: Corporate Compliance and Regulation. Oxford; New York: Oxford University Press 2007, lk 260.

puutumatusel.⁹² Andmekaitse direktiivis on see põhimõte sätestatud artikkel 6 lõike 1 punktis a – isikuandmeid töödeldakse õiglaselt ja seaduslikult. Selle põhimõtte üheks eesmärgiks on tagada, et isikuandmete töötlemine oleks lubatud vaid seaduses sätestatud alustel. Töösuhte puhul on seaduslikuks aluseks, mis annab tööandjale õiguse töötaja andmeid töödelda, töösuhete ise.⁹³ Andmekaitse direktiivi artikkel 7 punkt b sätestab, et isikuandmeid võib töödelda ainult juhul, kui töötlemine on vajalik sellise lepingu täitmiseks, mille osapool andmesubjekt on, või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele. See säte on harmoniseeritud IKS § 14 lg 1 p-s 4, mille kohaselt võib isikuandmeid töödelda andmesubjektiga sõlmitud lepingu täitmiseks või lepingu täitmise tagamiseks.

- Eesmärgikohasuse põhimõte – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas. See tähendab, et tööandja ei tohi andmeid töödelda lihtsalt igaks juhuks, vaid töötlemisel peab olema selgelt määratletud seaduslik eesmärk. Kui eesmärk ei ole seaduslik, on igasugune järgnev töötlemine ebaseaduslik. Eesmärk peab olema kindlaks määratud enne andmete kogumist ning sama eesmärgiga peab seonduma ka järgnev andmete töötlemine. See ei tähenda siiski, et eesmärgi muutmine oleks täiesti välistatud. Üldjuhul tuleb igal uuel eesmärgil töötlemiseks saada andmesubjektilt selgelt väljendatud nõusolek.⁹⁴

Andmekaitse direktiivi artikkel 6 lõike 1 punkt b kohaselt kogutakse isikuandmeid täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ega töödelda hiljem viisil, mis on vastuolus kõnealuste eesmärkidega.

Eesmärgi ja töödeldavate andmete täpne määratlemine teenib andmetöötluse läbipaistvuse eesmärki. Eesmärgi täpne sõnastamine on ühelt poolt vajalik tööandjale endale - selleks, et hinnata, kas planeeritav isikuandmete töötlemine on seaduslik ja proportsionaalne. Teiselt poolt on see vajalik töötajatele, kellel peab olema võimalus saada adekvaatne ülevaade isikuandmete töötlemisest. Kui isikuandmete töötlemise eesmärki pole võimalik tuvastada või sellest aru saada, on töötajal õigus IKS § 21 lg 1 kohaselt nõuda isikuandmete töötlemise lõpetamist.⁹⁵

⁹² E. Tikk, A. Nõmper, lk 92.

⁹³ M. Männiko, lk 143.

⁹⁴ E. Tikk, A. Nõmper, lk 92.

⁹⁵ Andmekaitse Inspeksioon, lk 18.

Isikuandmete töötlemine on vahend eesmärgi saavutamiseks ja seega ei saa olla andmete töötlemise eesmärgiks. Andmekaitse Inspeksiooni hinnangul ei ole sellised eesmärgi kirjeldused nagu „töötajate kontrollimiseks“, „töökohustuste täitmise kontrollimiseks“ või „turvalisuse tagamiseks“ piisavalt selgelt määratletud ja seega peab tööandja igal konkreetsel juhul määratlema, millise töökohustuse kontrollimiseks või millise turvariskiga seoses isikuandmeid töödeldakse.⁹⁶

- Minimaalsuse põhimõte – isikuandmeid võib koguda vaid ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks. Ulatuses all tuleb mõista ka ajalist ulatust, mis tähendab seda, et töötlemine tuleb lõpetada ja andmed kustutada või viia isikustamata kujule kohe, kui on täidetud eesmärgid, milleks nad koguti.⁹⁷ Vastavalt IKS § 24 p-le 1 on isikuandmete töötleja isikuandmete töötlemisel kohustatud eesmärkide saavutamiseks mittevajalikud isikuandmed viivitamata kustutama või sulgema, kui seadus ei näe ette teisiti.

Andmekaitse direktiivis on minimaalsuse põhimõtte sätestatud artikkel 6 lõike 1 punktis c - isikuandmed on piisavad, asjakohased ega ületa selle otstarbe piire, mille tarvis neid kogutakse ja/või hiljem töödeldakse, ja punktis e - isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik seoses andmete kogumise või hilisema töötlemise eesmärkidega.

- Kasutuse piiramise põhimõte – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal. See nõue väljendab andmete töötlemise eesmärgikohasuse põhimõtte teist poolt, võimaldades enne andmete kogumist kindlaksmääratud töötlemise eesmärkidest hiljem kõrvale kalduda vaid andmesubjekti nõusolekul.⁹⁸ Tööandja peab andmete kogumise eesmärgid enne koguma hakkamist määratlema ja teatavaks tegema. Kui ühtesid ja samu andmeid kogutakse mitme erineva eesmärgi täitmiseks, tulebki kõik eesmärgid eraldi ära nimetada. Kui otsustatakse, et ühel eesmärgil kogutavaid andmeid hakatakse kasutama ka muul eesmärgil, saab see kehtida ainult edaspidi kogutavate andmete osas, mitte aga tagasiulatuvalt juba kogutud andmete kohta.⁹⁹

⁹⁶ Andmekaitse Inspeksioon, lk 18.

⁹⁷ Andmekaitse Inspeksioon, lk 17.

⁹⁸ E. Tikk, A. Nõmper, lk 92.

⁹⁹ Andmekaitse Inspeksioon, lk 55.

- Andmete kvaliteedi põhimõte – isikuandmed peavad olema ajakohased, täielikud ning vajalikud seatud andmetöötluse eesmärgi saavutamiseks. Ühest küljest oleks põhjendamatu isikuandmete töötlemisel sekkuda isiku eraellu, kui kas kogutud andmete ebapiisavuse või nende ebatäpsuse või mitteajakohasuse tõttu jääks saavutamata see oluline töötlemise eesmärk, mis sellist isiku privaatsfääri sekkumist õigustanuks. Teisest küljest piirab see põhimõte aga isikuandmete kogumist suuremas ulatuses, kui andmetöötluse eesmärgi saavutamiseks vältimatult vajalik on.¹⁰⁰

IKS § 24 punktide 2 ja 3 kohaselt on isikuandmete töötleja isikuandmete töötlemisel kohustatud tagama, et isikuandmed on õiged ja, kui see on eesmärkide saavutamiseks vajalik, viimases seisus ning mittetäielikud ja ebaõiged isikuandmed sulgema ning nende täiendamiseks ja parandamiseks võtma viivitamata kasutusele vajalikud abinõud.

Vastavalt andmekaitseDirektiivi artikli 6 lõike 1 punktile d on andmed täpsed ja vajaduse korral ajakohastatud ning tarvitusele võetakse kõik mõistlikud meetmed, et kustutada või parandada andmete kogumise või hilisema töötlemise eesmärgi seisukohast ebaõiged või mittetäielikud andmed.

- Turvalisuse põhimõte – isikuandmete kaitseks tuleb rakendada turvameetmeid, et kaitsta neid tahtmatu või volitamata töötlemise, avalikuks tuleku või hävimise eest. Mida delikaatsemat laadi andmed ning mida suurem tahtmatu või volitamata töötlemise oht, seda tõhusamad peavad olema ka rakendatavad turvameetmed.¹⁰¹ Tööandja peab tagama, et töötajate isikuandmetele ei pääseks ligi töötajad, kel puudub selleks õigus ja vajadus. Samuti peavad töötajad, kes seoses oma töökohustuste täitmiseks töötlevad isikuandmeid, olema teadlikud isikuandmete töötlemise põhimõtetest ja pädevad selliste ülesannete täitmiseks.

AndmekaitseDirektiivis on turvalisuse põhimõte sätestatud artiklis 17, milles kehtestatakse muuhulgas, et liikmesriigid näevad ette, et vastutav töötleja peab rakendama vajalikke tehnilisi ja organisatsioonilisi meetmeid kaitsmaks isikuandmeid juhusliku või ebaseadusliku hävitamise või juhusliku kaotsimineku, muutmise, ebaseadusliku avalikustamise või juurdepääsu eest, eelkõige juhul, kui töötlemine hõlmab andmete edastamist võrgu kaudu, ning igasuguse muu võimaliku ebaseadusliku töötlemise eest.

¹⁰⁰ E. Tikk, A. Nõmper, lk 93.

¹⁰¹ E. Tikk, A. Nõmper, lk 93.

- Individuaalse osaluse põhimõte – andmesubjekti tuleb teavitada tema kohta kogutavatest andmetest, talle tuleb võimaldada juurdepääs tema kohta käivatele andmetele ja tal on õigus nõuda ebatäpsete või eksitavate andmete parandamist. Andmekaitseinspektsioonis on andmesubjekti teavitamine reguleeritud artiklites 10 ja 11 ning andmesubjekti õigust tutvuda andmetega käsitleb artikkel 12.

Isikuandmete töötlemise õigus ei tähenda töötleja absoluutset võimu andmete üle, andmesubjekt peab saama võimalikult palju oma isikuandmete töötlemist mõjutada, selles osaleda ja kontrollida. Inimene, kellel on selge ülevaade sellest, kes, kui palju ja milleks tema kohta andmeid kasutab, saab teadlikumalt oma käitumist juhtida ning oskab paremini teiste inimestega suhestuda. Teadmatus põhjustab ebakindlust ning seeläbi võivad saada kahjustada ka isiku muud õigused, eelkõige õigus vabale eneseteostusele.¹⁰²

Vastavalt IKS § 15 lg-le 1 peab isikuandmete töötleja juhul, kui isikuandmete allikaks ei ole andmesubjekt, pärast isikuandmete saamist, parandamist või enne isikuandmete edastamist kolmandale isikule tegema andmesubjektile viivitamata teatavaks töödeldavate isikuandmete koosseisu ja allikad ning andmed isikuandmete töötleja kohta. Kuigi seda selgesõnaliselt IKS-s pole välja toodud, tuleb lisaks avaldada ka andmete töötlemise eesmärk. Selle seisukohaga nõustub ka Andmekaitse Inspektsioon.¹⁰³ Samuti tuleneb see andmekaitseinspektsiooni artiklites 10 ja 11.

Kuigi IKS sätestab aktiivse teavitamiskohustuse andmete töötlejale ainult juhul, kui andmete allikaks ei ole andmesubjekt ise, siis andmekaitseinspektsiooni artikli 10 kohaselt on teavitamiskohustus ka siis, kui andmed kogutakse isikult endalt. Seega tuleks isikuandmete kogumisel andmesubjekti teavitada sõltumata sellest, kas andmed pärinevad andmesubjektilt endalt või muust allikast. Teavitamine peab olema selge ja ühemõtteline. Kuna seadusandja ei ole kehtestanud kirjalikus vormis teavitamise kohustust, siis võib teavitamine toimuda ka suuliselt.

Vastavalt IKS § 15 lg-le 2 ei ole vaja andmesubjekti isikuandmete töötlemisest teavitada, kui andmesubjekt on andnud nõusoleku oma isikuandmete töötlemiseks, kui andmesubjekt on juba töötlemisest teadlik, kui isikuandmete töötlemine on ette nähtud seaduses, kui andmesubjekti teavitamine ei ole võimalik või kui esinevad IKS-s toodud erakorralised

¹⁰² T. Ilus, lk 522.

¹⁰³ Andmekaitse Inspektsioon, lk 20.

asjaolud. Kuigi IKS § 15 lg 2 punkti 3 kohaselt ei pea isikuandmete töötlemisest teavitama juhul kui konkreetsete andmete kogumine on seaduses selgelt ette nähtud, siis IKS § 14 lg 1 p 4 alusel töölepingu täitmiseks andmete töötlemisel ei tulene seadusest, milliseid andmeid mis juhul täpselt töödeldakse ning seetõttu tuleb sellisest töötlemisest töötajat siiski teavitada.¹⁰⁴

Tulenevalt IKS § 19 lg-st 1 peab isikuandmete töötleja andmesubjekti soovil andmesubjektile teatavaks tegema tema kohta käivad isikuandmed, isikuandmete töötlemise eesmärgid, isikuandmete koosseisu ja allikad, kolmandad isikud, kellele isikuandmete edastamine on lubatud või kellele tema isikuandmeid on edastatud ning andmed isikuandmete töötleja kohta.

IKS § 21 lg 1 kohaselt on andmesubjektil õigus nõuda isikuandmete töötlejalt ebaõigete isikuandmete parandamist. Selle sätte eesmärk on kaitsta isikut väärade info levimise eest, mille põhjal omakorda võidakse langetada valesti kaalutud otsuseid isiku kohta. Lisaks ei ole sugugi väheoluline isiksusõiguse aspekt: isiku kohta väärkujutluse loomine valeandmete põhjal võib põhiseadusega kaitstud üldist isiksusõigust oluliselt riivata.¹⁰⁵

Seega peab tööandja töötajate isikuandmeid töödeldes olema kindel, et töötlemiseks on olemas õiguslik alus ning töötlemisel peetakse kinni isikuandmete töötlemise põhimõtetest. Kui neid nõudeid ei järgita, on tegu ebaseadusliku isikuandmete töötlemisega, mille eest tuleb tööandjal vastutada.

2.5 Tööandja vastutus isikuandmete töötlemisel

Tööandja peab isikuandmeid töödeldes olema teadlik ka vastutusest, mis kaasneb isikuandmete töötlemise nõuete rikkumisega. Andmekaitsealaste rikkumiste puhul on endise olukorra taastamine sageli võimatu. Küll aga on vastutusega võimalik andmesubjektile tekitatud kahju hüvitada, edasisi rikkumisi ära hoida ja rikkumise või kuriteo toimepanijat karistada.¹⁰⁶ Seega sõltuvalt toime pandud teo olemusest ja ulatusest võivad ebaseaduslikul isikuandmete töötlemisel ning töötaja privaatsusõiguse rikkumisel olla erinevad tagajärjed. Rikkumisele võivad järgneda Andmekaitse Inspektsiooni poolt kohaldatavad sanktsioonid. See võib kaasa tuua töötajapoolse töölepingu erakorralise ülesütlemise TLS § 91 lg 2 alusel

¹⁰⁴ Andmekaitse Inspektsioon, lk 55–56.

¹⁰⁵ T. Ilus, lk 525.

¹⁰⁶ M. Männiko, lk 85.

koos töötajale hüvitise maksmise kohustusega ning kohustuse hüvitada tekitatud kahju. Samas võib sellega kaasneda isegi karistusõiguslik vastutus.

Ennetamaks järgnevates alapeatükkides toodud rikkumisi ning sellega kaasnevat vastutust, peab tööandja tagama, et töötajad, kes vastutavad ettevõttes isikuandmete töötlemise eest, oleksid teadlikud isikuandmete töötlemise reeglitest ning saanud vastava väljaõppe. Soovitav oleks nende töötajate töölepingusse lisada ka konfidentsiaalsuskohustus. Samuti tuleks neid teavitada ebaseadusliku isikuandmete töötlemisega kaasnevatest võimalikest tagajärgedest nii neile endile, ettevõttele kui ka kaastöötajate privaatsusele. Ilma isikuandmeid töötlevate töötajate piisava koolitusega ei saa tööandja tagada, et ettevõtte töötajate privaatsust kohaselt austatakse.¹⁰⁷

2.5.1 Andmekaitse Inspektsiooni poolt kohaldatavad sanktsioonid

Eestis teostab andmekaitsealast riikliku järelevalvet Andmekaitse Inspektsioon. Andmekaitse Inspektsioonil on andmekaitsealase rikkumise korral vastavalt IKS § 33 lg 1 p-le 3 õigus alгатada vajaduse korral väärteomenetlus ja kohaldada karistust. IKS § 33 lg 2 alusel on Andmekaitse Inspektsioonil oma ülesannete täitmiseks õigus:

- peatada isikuandmete töötlemine;
- nõuda ebaõigete isikuandmete parandamist;
- keelata isikuandmete töötlemine;
- nõuda isikuandmete sulgemist või töötlemise lõpetamist, sealhulgas hävitamist või edastamist arhiivi;
- rakendada isiku õiguste ja vabaduste kahjustamise ärahoidmiseks vajaduse korral asendustäitmise ja sunniraha seaduses sätestatud korras viivitamata isikuandmete kaitseks organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid, välja arvatud juhul, kui isikuandmeid töötleb riigiasutus;
- nõuda isikutelt asjakohaseid dokumente ja muud vajalikku teavet ning teha dokumentidest koopiaid.

Lisaks on Andmekaitse Inspektsioonil IKS § 40 alusel õigus teha isikuandmete töötlejale ettekirjutusi ning nimetatud ettekirjutuse mittetäitmisel rakendada sunniraha. Isikuandmete

¹⁰⁷ Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context, lk 22.

töötajat võib karistada rahatrahviga delikaatsete isikuandmete töötlemise registreerimiskohustuse, isikuandmete kaitse turvameetmete või isikuandmete töötlemise muude nõuete eiramise eest (IKS § 42) ning isikuandmete kaitse turvameetmete või isikuandmete töötlemise muude nõuete rikkumise eest, kui isikule on rikkumise kõrvaldamiseks tehtud Andmekaitse Inspektsiooni poolt ettekirjutus ja seda ei ole täidetud (IKS § 42).

2.5.2 Töötajapoolne töölepingu erakorraline ülesütlemine ja kahju hüvitamine

Tööandja on vastavalt TLS § 28 lg 2 p-le 11 kohustatud austama töötaja privaatsust ja kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi. Samuti peab tööandja TLS § 41 lg 2 kohaselt tagama töötaja isikuandmete töötlemise vastavalt IKS-le. Kui tööandja töötleb ebaseaduslikult töötaja isikuandmeid ja rikub töötaja privaatsusõigust, siis on tööandja rikkunud töösuhtes talle TLS-ga pandud kohustusi. Olenevalt tööandja rikkumisest, võib töötaja pidada edasist töösuhte jätkumist võimatuks. Vastavalt TLS § 91 lg-le 2 võib töötaja töölepingu erakorraliselt üles öelda tööandjapoolse kohustuse olulise rikkumise tõttu, eelkõige kui tööandja on kohelnud töötajat ebaväärikalt või ähvardanud sellega või lubanud seda teha kaastöötajatel või kolmandatel isikutel (p 1) või töö jätkamine on seotud reaalse ohuga töötaja elule, tervisele, kõlbelisusele või heale nimele (p 3).

Kui töötaja ütleb töölepingu erakorraliselt üles põhjusel, et tööandja on lepingut oluliselt rikkunud, maksab tööandja töötajale TLS § 100 lg 4 alusel hüvitist töötaja kolme kuu keskmise töötasu ulatuses. Kohus või töövaidluskomisjon võib hüvitise suurust muuta, arvestades töölepingu ülesütlemise asjaolusid ja mõlema poole huvisid.

Kui tööandja on ebaseadusliku isikuandmete töötlemisega rikkunud töötaja õigusi, siis võib see kaasa tuua ka töötaja nõuded talle tekitatud varalise ja/või moraalse kahju hüvitamiseks. Andmekaitsealaseks rikkumiseks tuleb lugeda nii juhuseid, kui töödeldi (näiteks avaldati) andmesubjekti kohta ebaõigeid andmeid, kui ka neid juhuseid, kui töödeldavad andmed olid küll faktiliselt õiged, kuid töötlejal puudus õigus andmesubjekti isikuandmete töötlemiseks.¹⁰⁸

Kui tööandja eelnevalt nimetatud TLS-s sätestatud kohustusi ei täida, on tööandja rikkunud töölepingust tulenevaid omapoolseid kohustusi võlaõigusseaduse¹⁰⁹ (edaspidi VÕS) § 100

¹⁰⁸ M. Männiko, lk 85.

¹⁰⁹ Võlaõigusseadus. – RT I 2001, 81, 487 ... RT I, 08.07.2011, 21.

tähtenduses. Vastavalt VÕS §-le 100 on kohustuse rikkumine võlasuhtest tuleneva kohustuse täitmata jätmine või mittekohane täitmine, sealhulgas täitmisega viivitamine.

VÕS § 115 lg 1 sätestab, et kui võlgnik rikub kohustust, võib võlausaldaja koos kohustuse täitmisega või selle asemel nõuda võlgnikult kohustuse rikkumisega tekitatud kahju hüvitamist, välja arvatud juhul, kui võlgnik kohustuse rikkumise eest ei vastuta või kui kahju ei kuulu seadusest tulenevalt muul põhjusel hüvitamisele.

Vastavalt VÕS §-le 131 tuleb isikult vabaduse ebaseadusliku võtmise, isiku au teotamise või muu isikuõiguse rikkumisega tekitatud kahju hüvitamise kohustuse olemasolu korral kahjustatud isikule hüvitada talle põhjustatud kulutused, samuti hüvitada tema sissetuleku vähenemisest või edasiste majanduslike võimaluste vähenemisest tekkinud kahju. Selline kahju võib töötajale tekkida näiteks olukorras, kus tööandja on ebaseadusliku isikuandmete töötlemise tulemusena avalikustanud töötaja kohta teavet, mis raskendab töötajal leida edaspidi erialast tööd.

Mittevaralise kahju hüvitamist reguleerib VÕS § 134, mille lõike 1 kohaselt võib lepingust tuleneva kohustuse rikkumise eest mittevaralise kahju hüvitamist nõuda üksnes juhul, kui kohustus oli suunatud mittevaralise huvi järgimisele ning sõltuvalt lepingu sõlmimise või kohustuse rikkumise asjaoludest sai võlgnik aru või pidi aru saama, et kohustuse rikkumine võib põhjustada mittevaralise kahju. Antud juhul on eespool nimetatud tööandja kohustuste eesmärk kaitsta eelkõige töötaja privaatsust ja seega oleks mittevaralise kahju hüvitamise nõude esitamine õigustatud.

VÕS § 134 lg 2 sätestab, et isikult vabaduse võtmisest, isikule kehavigastuse tekitamisest, tema tervise kahjustamisest või muu isikuõiguse rikkumisest, sealhulgas isiku au teotamisest, tekkinud kahju hüvitamise kohustuse olemasolu korral tuleb kahjustatud isikule mittevaralise kahju hüvitiseks maksta mõistlik rahasumma. Vastavalt VÕS § 134 lg-dele 5 ja 6 arvestatakse mittevaralise kahju hüvitise määramisel rikkumise raskust ja ulatust ning kahju tekitaja käitumist ja suhtumist kahjustatud isikusse pärast rikkumist, lisaks võib kohus arvestada vajadust mõjutada kahju tekitajat hoiduma edasisest kahju tekitamisest, võttes seejuures arvesse kahju tekitaja varalist seisundit.

Seega peab tööandja arvestama, et eksimus töötajate isikuandmete töötlemise põhimõtete vastu ei pruugi põhjustada ainult töötajate usaldamatust tööandja suhtes ja halvendada

töösuhteid, vaid see võib viia ka töösuhte lõppemiseni ning tuua kaasa rahalise kohustuse hüvitada töötajatele tekitatud kahju.

2.5.3 Karistusõiguslik vastutus

Teatud juhtudel võib isiku privaatsusesse sekkumise negatiivne mõju olla puudutatud isiku elule ja tegevusele väga ulatuslik, seetõttu on mõned tegevused riigi poolt kriminaliseeritud ning vastavate tegude toimepanijaid võib oodata kriminaalkorras karistamine. On väga oluline, et nii tööandja kui ka ettevõttes otseselt isikuandmete ja nende töötlemisega kokkupuutuvad töötajad oleksid teadlikud nende tegevusega kaasnevast võimalikust karistusõiguslikust vastutusest, sest olenevalt rikkumisest ja teo toimepanija isiksusest, võivad toime pandud süüteo eest vastutada nii teo otseselt toime pannud isik kui ka juriidiline isik. Vastavalt karistusseadustiku¹¹⁰ (edaspidi KarS) § 14 lg-le 1 vastutab juriidiline isik seaduses sätestatud juhtudel teo eest, mis on toime pandud tema organi, selle liikme, juhtivtöötaja või pädeva esindaja poolt juriidilise isiku huvides. KarS § 14 lg 2 alusel ei välista juriidilise isiku vastutuselevõtmine süüteo toimepannud füüsilise isiku vastutuselevõtmist.

KarS § 137 alusel on karistatav eraviisiline jälitustegevus. Ebaseaduslikuks jälitustegevuseks on seadusliku õigusega isiku poolt teise inimese jälgimine tema kohta andmete kogumise eesmärgil. Eraviisilise jälitustegevuse eest karistatakse rahalise karistuse või kuni kolmeaastase vangistusega. Sama teo eest, kui selle on toime pannud juriidiline isik, karistatakse rahalise karistusega.

Eraviisilise jälitustegevusega rünnatav õigushüve on eneseteostusvabadus ja enesemääramisõigus, mis tulenevad otseselt PS §-st 19. KarS § 137 koosseisuga kaitstakse kõiki, sh elulisi ja tööalaseid andmeid, nende kvaliteet kuriteo toimepanija jaoks ei ole oluline. Asjaolu, et eraviisilise jälitustegevusega saadud andmed on liiga üldist laadi ega vastanud kuriteo toimepanija ootustele, ei vähenda vabadusevastase süüteo riive ulatust. Inimene ei saa olla oma otsustes vaba, kui ta teab, et iga ta sammu võidakse jälgida ja talletada.¹¹¹ Vastav koosseis võib katta ka töötajate ebaseadusliku jälgimise tööandja poolt.¹¹²

Jälgimisena mõistetakse isiku korduvat või pikemaajalist varjatud visuaalset vaatlemist vahetult või tehniliste seadmete abil, sõnumite salajast läbivaatamist või pealtkuulamist,

¹¹⁰ Karistusseadustik. – RT I 2001, 61, 364 ... RT I, 29.12.2011, 190.

¹¹¹ P. Pikamäe, J. Sootak. Karistusseadustik: kommenteeritud väljaanne. Tallinn: Juura 2009, § 137 komm 1.

¹¹² E. Tikk, A. Nõmper, lk 177.

sõltumata sõnumite edastamise, läbivaatamise või pealtkuulamise viisist ning asjade või inimese kohta andmeid sisaldavate andmekogude salajast läbivaatamist.¹¹³ Jälitustegevusena võib kvalifitseeruda ka n-ö liikluse jälgimine (st mitte sõnumite sisu, vaid neid iseloomustavad andmed): kes kellega suhtleb, kui mahukad on vahetatavad sõnumid, kui intensiivne on kommunikatsioon, kellele laekunud infot edastatakse jne.¹¹⁴

KarS § 156 kriminaliseerib sõnumisaladuse rikkumise. Kirjavahetuse ja sidevahendi abil edastatud sõnumi saladuse rikkumise eest karistatakse rahalise karistusega. Sama teo eest isiku poolt, kes pääses sõnumi juurde oma tööülesannete tõttu, karistatakse rahalise karistuse või kuni üheaastase vangistusega.

Antud normiga kaitstav õigushüve on igaühe põhiõigus määrata, kes võib sõnumiga tutvuda. Sõnum on igasugune kirjavahetus või sidevahendite abil edastatud informatsioon sõltumata andmekandjast. Sõnumil peab olema teatav isiklik side sõnumi saajaga. Sõnumi adressaat peab olema otseselt või kaudselt üheselt või sellega võrreldavalt piiritletud. Sõnumisaladus on kaitsmisväärne, kui saatja on püüdnud äratuntavalt ja kohaselt välistada sõnumi sisu teadasaamise kolmandatele isikutele. Sõnumisaladust on rikutud kui toimepanija on loonud võimaluse sõnumiga tutvumiseks endale või kolmandatele isikutele. Sõnumi edastamine ei pea olema lõpule viidud, sõnumisaladust on rikutud ka sõnumi saatmise alustamise takistamise või sõnumi peatamisega. Antud süüteo subjektiks saab olla isik, kellele sõnum ei olnud teo toimepanemise ajal suunatud. Isiku, kellele sõnum on suunatud, määrab sõnumi koostaja adressaadina. Alates sõnumi jõudmisest adressaadi sfääri määrab adressaat isiku, kellele sõnum on suunatud.¹¹⁵

KarS § 157 kohaselt on karistatav kutse- ja ametitegevuses teatavaks saanud saladuse hoidmise kohustuse rikkumine. Kutse- või ametitegevuses teatavaks saanud teise isiku tervist, eraelu või äritegevust puudutava teabe avaldamise eest isiku poolt, kellel on seadusest tulenev kohustus hoida sellist teavet saladuses, karistatakse rahalise karistusega või kuni kolmeaastase vangistusega.

¹¹³ P. Pikamäe, J. Sootak, § 137 komm 3.3.

¹¹⁴ E. Tikk, A. Nõmper, lk 177–178.

¹¹⁵ P. Pikamäe, J. Sootak, § 156 komm 1, 2.

Nimetatud paragrahviga kaitstav õigushüve on informatsiooniline enesemääramise õigus ja eraelu kaitse. Süüteo koosseisu eesmärk on võimaldada usaldusel põhineva suhte loomine olukorras, kus üks isik peab teisele isikule avaldama konfidentsiaalset informatsiooni.¹¹⁶

Kutse- või ametitegevuses teatavaks saamine tähendab, et isik ei oleks saladust teada saanud, kui tal ei oleks vastavat kutse- või ametiseisundit. Saladuses hoitav teave on igasugune faktiline asjaolu, mis ei ole teada üldiselt, vaid ainult väga piiratud inimesteringile ja mille saladuses hoidmiseks on isikul õigustatud huvi. Saladuses hoitav teave peab käima tervise, eraelu või äritegevuse kohta. Tervis hõlmab igasuguseid andmeid inimese genotüübi ja fenotüübi kohta. Eraelu hõlmab isiku tervet isiklikku elusfääri, kogu privaatse elukorralduse autonoomset valdkonda, milles isik oma individuaalsust arendab ja säilitab. Äritegevus hõlmab andmeid isiku majandusliku olukorra ja potentsiaali kohta. Avaldamine on teabe teatavastegemine teadasaamiseks mitteõigustatud isikutele.¹¹⁷

Lisaks on KarS § 157¹ alusel karistatav delikaatsete isikuandmete ebaseaduslik avaldamine. Delikaatsete isikuandmete ebaseadusliku avalikustamise, andmetele juurdepääsu võimaldamise või andmete edastamise eest omakasu eesmärgil või kui sellega on tekitatud oluline kahju teise isiku seadusega kaitstud õigustele või huvidele karistatakse rahalise karistuse või kuni üheaastase vangistusega.

Samuti peab tööandja arvestama sellega, et kui ta soovib koguda tõendeid tõendamaks töötaja töökohustuste rikkumist, siis vastavalt tsiviilkohtumenetluse seadustiku¹¹⁸ § 238 lg 3 p-le 1 võib kohus keelduda tõendi vastuvõtmisest ja selle tagastada, kui tegemist on kuriteoga või põhiõiguse õigusvastase rikkumisega saadud tõendiga.

Töösuhetes on isikuandmete töötlemine möödapääsmatu ja tööandjad puutuvad sellega kokku igapäevaselt. Seetõttu on isikuandmete töötlemine töösuhetes muutunud suhteliselt tavapäraseks tegevuseks ning alati ei pruugita endale teadvustadagi, et tegu on isikuandmete või nende töötlemisega. See omakorda võib tuua kaasa eksimise seadusandja poolt isikuandmete töötlemise piiramiseks kehtestatud reeglite vastu. Seega ei pea tööandja tagama ainult seda, et ta ise ettevõtte tööd korraldades andmekaitse põhimõtteid järgiks, vaid ka seda, et ettevõttes otseselt isikuandmetega kokkupuutuvad töötajad oleksid nendest põhimõtetest teadlikud ning ei paneks tahtlikult või teadmatusel toime andmekaitsealaseid rikkumisi.

¹¹⁶ P. Pikamäe, J. Sootak, § 157 komm 1.

¹¹⁷ P. Pikamäe, J. Sootak, § 157 komm 2.

¹¹⁸ Tsiviilkohtumenetluse seadustik. – RT I 2005, 26, 197 ... RT I, 28.12.2011, 44.

3. TÖÖTAJA PRIVAATSUSE PIIRAMINE TÖÖSUHETES

3.1 Töötaja kontrollimine

Tööandja õigus töötajat kontrollida tuleneb juba töösuhte ja töölepingu olemusest. TLS § 1, avades töölepingu mõiste, sätestab, et töölepingu alusel teeb füüsiline isik (töötaja) teisele isikule (tööandja) tööd, alludes tema juhtimisele ja kontrollile. Tööandja kontrolliõigus on vajalik tagamaks töötajate korrektset ja efektiivset tööülesannete täitmist, mis omakorda on aluseks edukale äritegevusele ja ettevõtte toimimisele. Samas peab tööandja arvestama TLS § 28 lg 2 p-ga 11, millest tulenevalt on tööandja kohustatud austama töötaja privaatsust ja kontrollima töökohustuste täitmist viisil, mis ei riku töötaja põhiõigusi.

Antud töös käsitletakse töötaja kontrollimise teemat tavapärasest natuke laiemalt, hõlmates ka töötaja joobeseisundi tuvastamise ning töötaja töövõimetuse ja tervisekontrolliga seotud probleeme. Kuna ka need küsimused on väga tihedalt seotud töötaja privaatsusega ning kaudselt käsitatavad töötaja kontrollimisena tööandja poolt.

Töötaja kontrollimise esemeks saavad olla vaid tööga seotud asjaolud. Töötaja töövälisest tegevusest võib tööandja kontrollida ainult töösuhtega seotud asjaoludel. Näiteks võib töövälise tegevuse kontrollimine kõne alla tulla seoses TLS § 15 lg 2 p-s 9 sätestatud töötaja kohustusega hoiduda tegudest, mis kahjustavad tööandja mainet või põhjustavad klientide või partnerite usaldamatust tööandja vastu. Kõiki kontrollitavaid asjaolusid peab olema võimalik seostada töötaja töökohustustega, sest tööandja õigus kontrollida saab eksisteerida vaid juhul, kui töötajal on vastav kohustus.¹¹⁹ Töötajale kehtestatud nõuded ja kohustused, mille täitmist on tööandjal õigus kontrollida, tulenevad eelkõige töölepingust, kollektiivlepingust, tööandja poolt kehtestatud töökorraldusreeglitest ning seadusest.

Põhiõigused, millega tööandja vastavalt TLS § 28 lg 2 p-le 11 töötaja kontrollimisel arvestama peab, on eelkõige käesoleva töö esimeses peatükis käsitletud põhiõigused: õigus eraelu puutumatusele, õigus vabale eneseteostusele, õigus sõnumisaladusele ja õigus väljendusvabadusele. Kuna igasugune andmete kogumine riivab töötaja eraelu puutumatust, siis ei ole töötaja kontrollimine võimalik ilma tema põhiõigusi riivamata. Seega tuleb TLS §

¹¹⁹ Andmekaitse Inspektsioon, lk 52.

28 lg 2 p-s 11 nimetatud põhiõiguste rikkumise all silmas pidada põhiõiguste ülemäärast riivet.¹²⁰

Eraelu puutumatus kaitsealas on ka inimese füüsiline puutumatus. Seda tuleb arvestada selliste kontrollimeetmete rakendamisel nagu isiku ja tema asjade füüsiline läbivaatus. Sellised kontrollimeetmed võivad riivata ka üldisemat inimväärikuse austamise nõuet.¹²¹ Inimväärikus on PS-e üks aluspõhimõtetest, seega üks kõige olulisem väärtus Eesti õiguskorras üldse. Nii peab tööandja lisaks põhiseaduses selgesõnaliselt põhiõigustena defineeritud õigustele austama töötaja kontrollimisel alati ka töötaja inimväärikust.¹²² Riigikohus on oma lahendis öelnud, et inimkeskses ühiskonnas tohib põhiõiguste konfliktiolukordades kõige vähem piirata inimväärikust – kompleksset põhiõigust, mille elementideks on eeskätt õigus heale nimele, õigus mitte olla hirmul enese ja oma lähedaste eksistentsi pärast, õigus õiguslikule võrdsusele kõigi teiste inimestega, õigus inimlikule identiteedile, informatsioonilise enesemääramise õigus, õigus kehalisele puutumatusse.¹²³

Mitte ainult töötaja füüsiline läbivaatus ei ohusta töötaja inimväärikust, vaid tööandja peab arvestama, et ka ebaseaduslik jälgimine rikub töötaja inimväärikust.¹²⁴ Töötaja läbiotsimise käigus toimub ka väga ulatuslik isikuandmete töötlemine, kuna töötaja või tema asjade läbiotsimise käigus saadakse töötaja kohta täiendavat informatsiooni. Kui sellisele kontrollimeetmele peaks leiduma õigustus, siis tuleb väga rangelt järgida saadud info edasise kasutamise piiranguid. Läbivaatuse eesmärgiga mitteseotud info edasine töötlemine ükskõik millisel viisil on keelatud.¹²⁵

Töötajaid kontrollides peab tööandja arvestama käesoleva töö alapeatükis 2.4 käsitletud isikuandmete töötlemise põhimõtetega ja sellest tulenevalt peab tööandja sõltumata kontrollimise meetodist enne kontrollimist selgelt ja täpselt määratlema kontrolli eesmärgi. Eesmärgi saavutamiseks valitud kontrollimeetmete ning sellega kaasnev võimalik töötaja privaatsuse riive peab olema soovitava eesmärgiga proportsionaalne. Mida intensiivsemalt kontrollimeetmete töötaja õigusi riivab, seda mõjuvamad peavad olema tööandja põhjused selle läbiviimiseks. Samuti peab töötaja olema kontrollimisest teadlik ning tal peab olema soovi korral võimalus selle käigus kogutud teabega tutvuda.

¹²⁰ Andmekaitse Inspeksioon, lk 53.

¹²¹ Andmekaitse Inspeksioon, lk 53.

¹²² Andmekaitse Inspeksioon, lk 10.

¹²³ RKKKo 3-1-1-80-97.

¹²⁴ Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne, § 10 komm 3.1.4.

¹²⁵ Andmekaitse Inspeksioon, lk 53.

3.1.1 Töötaja kontrollimise meetodid

Kuna seadus reeglina ei sätesta, mil viisil tööandja teatud asjaolusid ning töötaja töökohustuste täitmist täpselt kontrollida võib, siis on tööandjal töötaja kontrollimiseks võimalik kasutada väga erinevaid meetmeid ja nende meetmete riive töötaja põhiõigustele on samuti väga erinev.

Kõige vähem riivavamad on töötaja jaoks kindlasti meetodid, mille puhul tööandja küsib tööülesannete täitmise või muude asjaolude kontrollimiseks andmeid töötajalt endalt või palub tal esitada vastavad dokumendid selle tõendamiseks.

Tööandja saab töötajaid kontrollida ja nende pädevust hinnata ka kaastöötajate kaasabil, näiteks küsides neilt teavet teatud konkreetse tööülesande täitmise kohta või paludes neil hinnata kolleegi võimet tulla toime oma tööülesannete täitmisega. Samuti on võimalik töötajate pädevust lasta hinnata konkreetse eriala koolitajatel ning ekspertidel, võimaldades neil töötajate sobivuse ja pädevuse hindamiseks läbi viia erinevaid eksameid või teste.

Seejuures ei tohi unustada, et ka sellisel juhul on tegu töötaja isikuandmete töötlemisega, kuna isikuandmed sisalduvad ka subjektiivsetes arvamustes ja hinnangutes, kuivõrd need hõlmavad andmeid isiku füüsiliste, psühholoogiliste, majanduslike, kultuuriliste ja sotsiaalsete omaduste kohta. See kehtib ka juhul, kui hinnang on väljendatud skoori või hindena või muu hindamiskriteeriumina.¹²⁶ Rahvusvahelise Tööorganisatsiooni (edaspidi ILO) 1997. aastal vastu võetud koodeks töötaja isikuandmete kaitse kohta,¹²⁷ mis sätestab, et töötaja võib isiksuse- ja muudest sarnastest testidest keelduda. Seega tohib teste läbi viia ainult töötaja nõusolekul. Olgu öeldud, et nimetatud ILO koodeks ei ole siiski liikmesriikidele otsekohaldatav, vaid pigem soovituslik abimaterjal seaduste väljatöötamisel ja tõlgendamisel.

Soomes võib töötaja nõusolekul läbi viia isiksuse ja sobivuse hindamise teste, selgitamaks välja töötaja võimekust täita tööülesandeid või koolitusvajadust ja kutsealast arengut.

¹²⁶ Article 29 Data Protection Working Party. Recommendation 1/2001 on Employee Evaluation Data. Arvutivõrgus: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp42en.pdf>, 03.02.2012.

¹²⁷ International Labour Office Code of practice on the protection of workers' personal data, p 6.11. Arvutivõrgus: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf, 15.01.2012.

Tööandja peab tagama, et kasutatavad hindamismeetodid oleksid usaldusväärsed, hindamist viiksid läbi oma ala eksperdid ning hindamistulemused ei sisaldaks vigu.¹²⁸

Seega peaks tööandja vältima selliseid üldisi isiku vaimset võimekust ja isikuomadusi mõõtvaid ning otseselt töökohustega mitte seotud teste. Tööandja peaks eelistama töötaja kontrollimisel ja hindamisel meetodeid, mis on seotud konkreetset tema tööülesannete täitmisega, näiteks hindama töötaja tööülesannete täitmiseks kasutatava arvutiprogrammi tundmist ja kasutamisoskust.

Töötajate kontrollimist võimaldavad ka erinevad tehnilised lahendused ja seadmed. Üheks selliseks võimaluseks on uksekaardisüsteem, kus ettevõtte ukseks avanevad ainult töötajale tööandja poolt väljastatud personaalset uksekaarti kasutades. Selle kaudu on võimalik kontrollida töötaja tööajast kinnipidamist, kuna need kaardid fikseerivad töötaja tööle saabumise ja töölt lahkumise kellaaja, samuti on võimalik vastava seadistuse korral selle süsteemi kaudu jälgida ka töötaja ettevõttesisest liikumist. Tööandjale kuuluvate sõidukite liikumist on võimalik jälgida sõidukisse paigutatud GPS-seadme kaudu.

Kõige rohkem riivavad töötaja privaatsust kindlasti kontrollimise viisid, mis seisnevad töötaja, tema asjade või töökoha läbiotsimises ning samuti töötaja jälgimises. Kuna töötaja või tema asjade läbiotsimine toob kaasa väga intensiivse sekkumise töötaja privaatsusesse, saab selline kontrollimise meetod päevakorda tulla ainult äärmisel vajadusel. Seda kinnitab ka see, et näiteks TLS-i seletuskirjas peetakse TLS § 28 lg 2 p-s 11 nimetatud privaatsuse austamise all silmas keeldu otsida läbi töötaja kabinetti või kuulata pealt telefonikõnesid.¹²⁹

Tööandja võib töötajat kontrollida ka läbi arvuti ja muude kommunikatsioonivahendite kasutamise jälgimise või paigaldada selleks spetsiaalsed jälgimisseadmed (näiteks turvakaamerad).

UK juhise kohaselt peab kontrollimise negatiivne mõju töötajatele olema õigustatud tööandja või teiste isikute kasuga. Sellest lähtudes tuleb tööandjatel enne otsustamist, kas ja kuidas töötajaid kontrollida, viia läbi selle mõju hindamine. Selle abil saab tööandja otsustada, kas kontrollimeede on proportsionaalne reageering probleemile, mida püütakse lahendada. Mõju hindamisel tuleb:

¹²⁸ Act on the Protection of Privacy in Working Life, section 13.

¹²⁹ Seletuskiri töölepingu seaduse eelnõu juurde, lk 31. Arvutivõrgus: http://www.riigikogu.ee/?page=en_vaade&op=ems&eid=353198&u=20090309131308, 06.02.2012.

- määratleda selgelt kontrollmeetme eesmärk ja kasu, mis sellega kaasneb;
- määratleda kontrollmeetme negatiivne mõju töötajatele ja teistele isikutele (näiteks klientidele);
- kaaluda alternatiivseid võimalusi kontrollimiseks sama eesmärgi saavutamiseks;
- võtta arvesse kohustusi, mis kaasnevad kontrollimisega (näiteks töötajate teavitamine, kontrollimise käigus kogutud andmete töötlemine ja säilitamine);
- otsustada, kas kontrollimine on õigustatud.¹³⁰

Töötajate kontrollimise meetodite ja ulatuse üle otsustades peaks tööandja kindlasti kaaluma ka seda, kas neid meetmeid rakendada kõikidele töötajatele või piirduda ainult nende töötajate kontrollimise ja jälgimisega, kelle suhtes on tööandjal kahtlusi või kelle peale on tulnud klientidelt kaebusi.

3.1.2 Delikaatsed isikuandmed töötaja kontrollimisel

IKS § 14 lg 1 p 4 kohaselt ei või lepingu täitmise eesmärgil töödelda delikaatseid isikuandmeid. Seega delikaatseid isikuandmeid võib tööandja töötaja kontrollimise käigus töödelda juhul, kui selline õigus tuleneb tööandjale seadusest või kui töötaja annab selleks nõusoleku.¹³¹ Töösuhetes ettetulevad olukorrad, kus tööandja puutub töötaja kontrollimisel kokku töötaja delikaatsete isikuandmetega, on näiteks töötaja ebakaines olekus tööle ilmunine, töövõimetuslehel viibimine ja töötaja tervisekontrolli korraldamine.

3.1.2.1 Joobeseisund

Vastavalt töötervishoiu ja tööohutuse seaduse¹³² (edaspidi TTOS) § 13 lg 1 p-le 15 on tööandja kohustatud kõrvaldama töölt alkoholi-, narkootilises või toksilises joobes või psühhotroopse aine mõju all oleva töötaja. TLS § 88 lg 1 p 4 kohaselt on tööandjal õigus töötajaga tööleping erakorraliselt üles öelda, kui töötaja on tööandja hoiatusest hoolimata viibinud tööl joobeseisundis. Õiguslikult käsitatakse joobeseisundit kui terviseseisundit ja andmed terviseseisundi kohta on vastavalt IKS-le delikaatsed isikuandmed.¹³³ Riigikohus on alkoholi tarvitamisest põhjustatud joobeseisundit defineerinud kui terviseseisundit, mis avaldub väliselt tajutavates häiritud või muutunud kehalistes või psüühilistes funktsioonides

¹³⁰ Information Commissioner's Office. The Employment Practices Code, lk 60–62.

¹³¹ Andmekaitse Inspeksioon, lk 52.

¹³² Töötervishoiu ja tööohutuse seadus. – RT I 1999, 60, 616 ... RT I, 10.02.2012, 5.

¹³³ RKHKo 3-3-1-98-06.

ja reaktsioonides.¹³⁴ Kuivõrd psühhotroopne aine mõjutab samuti tervises seisundit, on andmed selle tarvitamise kohta samamoodi delikaatsed isikuandmed.¹³⁵

Kui tööandjal tekib kahtlus, et töötaja on tööle tulnud ebakaines olekus, siis millised on tööandja võimalused töötaja joobeseisundit kontrollida ja tõendada. Kui tööandja eemaldab joobe kahtlusega töötaja töölt või lõpetab temaga töölepingu ilma joobetunnuseid korrektselt tuvastamata ja dokumenteerimata, võib töötaja pidada oma töölt kõrvaldamist põhjendamatuks ning nõuda töölt eemaloldud aja eest töötasu või vaidlustada töölepingu ülesütlemine ja nõuda töölepingu ülesütlamise tühisuse korral ettenähtud hüvitist. Seega on joobe tuvastamine sellises olukorras väga oluline, kuid ükski õigusakt vastavat korda ei kehtesta.

Riigikohus on oma lahendiga, mis puudutas küll avalikku teenistust, kuid mis võiks analoogia korras olla kohaldatav ka töösuhetes, andnud juhised joobeseisundi tuvastamiseks. Avaliku teenistuse seaduse¹³⁶ § 84 p-s 1 sätestatud koosseisu tunnus "teenistuses joobnuna viibimine" ei eelda kindlat alkoholikontsentratsiooni veres ega väljahingatavas õhus ehk puudub numbriline piirmäär, mille tuvastamisel saaks automaatselt käsitada isikut joobnud olekus olevana. Samas eeldab joobnud olek isiku tüüpiliste kehaliste või psüühiliste funktsioonide või reaktsioonide muutumise või häirumise tuvastamist. Üksnes indikaatorvahendi numbriline näit ei ole joobnud oleku tuvastamisel lõplikult määrava tähendusega. Siiski võib indikaatorvahendi kasutamisega tuvastatud joobnud olekule iseloomulik numbriline tulemus olla üheks isiku joobnud olekut kinnitavaks tõendiks. „Teenistuses joobnuna viibimine“ on tuvastatav tõendamise üldiste reeglite järgi ning selle tuvastamine on põhimõtteliselt võimalik ka üksnes alkoholi tarvitamisest tingitud isiku tüüpiliste kehaliste või psüühiliste funktsioonide või reaktsioonide muutumise või häirumise tuvastamise kaudu. Joobnuna teenistuses viibimise tõendamiseks võib seega kasutada menetlusosalise seletusi, dokumentaalseid tõendeid, asitõendeid, tunnistaja ütluseid, eksperdi arvamust, aga ka mõõtevahendi kasutamisel saadud tulemusi.¹³⁷

Üheks tööandjate poolt praktikas rakendust leidnud võimaluseks on kutsuda kohale politsei, sest vastavalt politsei ja piirivalveseaduse¹³⁸ §-le 7²³ võib politsei kontrollida isiku organismis alkoholi, narkootilise või psühhotroopse aine või muu sarnase toimega aine esinemist ja sama

¹³⁴ RKHKo 3-3-1-45-11.

¹³⁵ Andmekaitse Inspeksioon, lk 43.

¹³⁶ Avaliku teenistuse seadus. – RT I 1995, 16, 228 ... RT I, 29.12.2011, 166.

¹³⁷ RKHKo 3-3-1-45-11.

¹³⁸ Politsei ja piirivalveseadus. – RT I 2009, 26, 159 ... RT I, 29.12.2011, 28.

paragrahvi punktile 2 allutada joobeseisundi kontrollimise või tuvastamise protseduurile isiku, kellel esinevad ilmsed joobeseisundi tunnused, kui ta võib olla ohtlik endale või teistele. Sõltuvalt töötaja joobeastmest ja tema tööülesannete iseloomust, võib ebakaines olekus tööl viibimine olla ohtlik nii töötajale endale kui tema kaastöötajatele. Joobeseisundis töötajal on tööõnnetusse sattumise riski tunduvalt suurem, kuna muuhulgas halvendab joove töötaja reaktsioonikiirust ja koordineerimist.

Tööandjate poolt praktikas joobe tuvastamiseks ja tõendamiseks kasutatavatest meetoditest võib veel välja tuua alkomeetri kasutamise, töötaja arsti juurde saatmise ning teiste kaastöötajate tunnistajatena kasutamise, kes hindavad töötaja joovet väliste joobe tunnuste esinemise põhjal. Tööandja võib joobe kahtlusega töötajale teha ettepaneku alkomeetrisse puhumiseks või arsti juurde minekuks, kuid füüsiliselt ta töötajat selleks sundida ei saa, kuna lisaks isikuandmete kaitse küsimusele tekib siin vastuolu ka isiku füüsilise enesemääramise õigusega.¹³⁹

Andmekaitse Inspeksioon on seisukohal, et töötaja saatmist arsti juurde tuleks eelistada sellele, et tööandja kutsub „ilmingutega“ töötajat üle vaatama teised töötajad. Kuna erinevalt ettevõtte töötajatest töötleb arst delikaatseid isikuandmeid seaduse alusel ning tal on seadusest tulenev saladuse hoidmise kohustus. Ettevõtte teiste töötajate spetsiaalselt kohale kutsumine ei ole kooskõlas IKS-ga, sest tööandjal ei ole IKS § 14 lg-st 2 tulenevalt alust levitada joobes töötaja kohta delikaatseid isikuandmeid. Tunnistajatena saaks tööandja IKS-i kohaselt kasutada neid töötajaid, kes ise on joobes töötajaga kokku puutudes tajunud olukorda, ilma et tööandja oleks neid selleks eraldi kohustanud. Tööandja võib siiski informeerida töötaja joobeseisundist ning vajadusel kasutada ka tunnistajana töökeskkonnavolinikku, sest TTOS-e kohaselt on töökeskkonnavoliniku kohustus seista hea selle eest, et töökeskkond oleks ohutu.¹⁴⁰

Tööandja poolt kehtestatud korda töötajate kontrollimiseks alkomeetriga iga tööpäeva alguses, ei saa pidada andmekaitse seisukohalt lubatavaks. Kuigi TTOS § 13 lg 2 annab tööandjale õiguse kehtestada ettevõttes seadusega võrreldes rangemad töötervishoiu ja tööohutuse nõuded ja kontrollida nende täitmist, siis isegi kui selliseid meetmeid saab pidada tööohutuse nõueteks, peab arvestama, et igasugune tervises seisundi kontroll riivab isiku füüsilist enesemääramisõigust ning toob kaasa delikaatsete isikuandmete töötlemise.

¹³⁹ Andmekaitse Inspeksioon, lk 44.

¹⁴⁰ Andmekaitse Inspeksioon, lk 44–45.

Andmekaitse Inspektsiooni hinnangul ei ole TTOS-e sätted piisavalt selged selleks, et neid saaks käsitleda IKS § 10 lg 1 mõttes seadusliku alusena isikuandmete töötlemiseks olukorras, kus ei esine joobe ilminguid. Isegi kui seaduslik alus oleks olemas, tuleks vastavalt TLS § 28 lg 2 p-le 11 hinnata, kas selline kontrollimeetod on proportsionaalne konkreetse töökoha riske arvestades.¹⁴¹

Soomes ja Suurbritannias on lubatud alkoholi- ja narkotestid, kuid seda ainult juhul, kui see on vajalik ohutuse tagamiseks. Soomes võib tööandja nõuda töötajalt narkotesti tõendi esitamist, kui tal on põhjendatud alus kahtlustada, et töötaja on tööl olles narkojoobes või et tal on narkosõltuvus ning testimine on hädavajalik, et selgitada välja töötaja töövõime ning töötaja teeb tööd, mis nõuab erilist täpsust, usaldusväärsust, iseseisvaid otsuseid või kiiret reaktsiooni ning töötamine narkootilise aine mõju all või olles narkosõltuvuses võib kaasa tuua seaduses loetletud tagajärjed, nagu näiteks ohustada töötaja või teiste isikute elu, tervist või tööohutust. Narkotesti väljastavad tööandja poolt määratud tervishoiutöötaja ja labor. Tööandja võib määrata mõistliku tähtaja nimetatud tõendi esitamiseks.¹⁴²

Seega seni, kuni seadusandja pole kehtestanud töösuhetes joobeseisundi tuvastamise korda, siis tuginedes eespool toodule, oleks tööandjal mõistlik töötaja joobe kahtluse korral esmalt fikseerida töötaja välised joobe tunnused (näiteks ebakindel kõnnak, tasakaaluhäired, segane kõne). Töötaja joobe ilminguid võiks tõendada tunnistajate ütlustega, kelleks oleks joobes töötajaga kokkupuutunud kaastöötajad ning vajadusel töökeskkonnaspetsialist või töökeskkonnavolinik. Töötaja nõusolekul tuleks töötajal lasta joobe taseme mõõtmiseks puhuda alkomeetrisse, mis peab olema taadeldud ja identifitseeritav, või suunama ta joobe tuvastamiseks meditsiini-asutusse. Kui olukord on tõeliselt kriitiline ning ebakaines olekus töötaja on endale või teistele ohtlik (näiteks on töötaja vägivaldne), kutsuma kohale politsei.

3.1.2.2 Ajutine töövõimetus

Töötajal on õigus keelduda töö tegemisest, kui ta on ajutiselt töövõimetu ja viibib arsti poolt väljastatud töövõimetuslehel (TLS § 19 p 2). Töötaja peab tööandjat oma ajutisest töövõimetusest ja selle eeldatavast kestusest teavitama esimesel võimalusel (TLS § 15 lg 1 p10).

¹⁴¹ Andmekaitse Inspektsioon, lk 45.

¹⁴² Act on the Protection of Privacy in Working Life, section 6, 8.

Paraku tuleb ette juhuseid, kus töötaja kuritarvitab tööandja usaldust ja kasutab töövõimetuslehte ettekäändena vabade päevade saamiseks. Kui tööandjal tekib kahtlus, et töötaja, kes viibib töövõimetuslehel, tegelikult ei ole haige, siis on loomulik, et tööandja soovib kontrollida, kas töötajale töövõimetuslehe väljastamine on ikka põhjendatud. Seda enam, et 4. kuni 8. haiguslehel viibimise päeva eest on töötajale haigushüvitusi maksmise kohustust tööandjal. Samas tööandjal sellist õigust ei ole, ta peab usaldama haiguslehe väljastanud arsti, sest ravikindlustuse seaduse¹⁴³ § 52 lg 2 teise lause alusel vastutab töövõimetuslehe väljastaja ajutise töövõimetuslehe kindlustusjuhtumi õigesti määramise ja ajutise töövõimetuslehe põhjendatuse eest. Tööandjal on õigus esitada haigekassa piirkondlikule osakonnale avaldus haiguslehe väljaandmisega seotud asjaolude kontrollimiseks, sest haigekassa usaldusarstidel on Eesti Haigekassa seaduse¹⁴⁴ § 4 lg 1 alusel õigus kontrollida töövõimetuslehtede õigsust ja põhjendatust.¹⁴⁵

Andmekaitse Inspeksioon on seisukohal, et kontrolli läbiviimise tulemuste kohta on tööandjal õigus teada saada, kas töövõimetuslehe väljaandmine oli põhjendatud või mitte või kas tuvastati hüvitise maksmisest keeldumise alus. IKS § 14 lg 2 p 1 kohaselt võib Eesti Haigekassa väljastada tööandjale konkreetse töötaja töövõimetuslehega seotud andmeid, sest tööandja töötleb töövõimetuslehega seonduvaid isikuandmeid seadusega ettenähtud ülesande täitmiseks. Tööandjale seadusest tulenevaks ülesandeks on haigushüvitise maksmine. Haigekassa poolt kontrolli teostamise tulemuste kohta andmete väljastamine on tööandjale vajalik seetõttu, et töövõimetusleht on tööandjale haigushüvitise maksmise aluseks olev dokument. Muid andmeid, st diagnoosi, raviskeemi vms kohta tööandjale väljastada ei tule.¹⁴⁶

3.1.2.3 Tervisekontroll

Vastavalt TTOS § 13 lg 1 p-le 7 peab tööandja korraldama tervisekontrolli töötajatele, kelle tervist võib tööprotsessi käigus mõjutada töökeskkonna ohutegur või töö laad, ning kandma sellega seotud kulud. Töökohal töötajat mõjutada võivad ohutegurid määratakse kindlaks töökeskkonna riskianalüüsis. TTOS § 13 lg 1 p-st 3 tulenevalt korraldab tööandja töökeskkonna riskianalüüsi, mille käigus selgitatakse välja töökeskkonna ohutegurid, mõõdetakse vajaduse korral nende parameetrid ning hinnatakse riske töötaja tervisele ja ohutusele, arvestades tema ealisi ja soolisi iseärasusi, ning töökohtade ja töövahendite

¹⁴³ Ravikindlustuse seadus. – RT I 2002, 62, 377 ... RT I, 10.06.2011, 8.

¹⁴⁴ Eesti Haigekassa seadus. – RT I 2000, 57, 374 ... RT I, 23.12.2011, 7.

¹⁴⁵ Haigekassa THV maksmise kord: küsimused ja vastused. Arvutivõrgus: <http://www.haigekassa.ee/tooandjale/tvh-maksmise-kord-kysimu>, 12.02.2012.

¹⁴⁶ Andmekaitse Inspeksioon, lk 43.

kasutamise ja töökorraldusega seotud riske. Seega sõltub töötaja tervisekontrolli vajadus töökeskkonna riskianalüüsi tulemusest, millest selgub, kas antud töökohal ohustavad töötajat töökeskkonna ohutegurid või töö laad.

Kui riskianalüüsist selgub, et ohutegurite mõju töötajale on olemas ja tööandja suunab töötaja tervisekontrolli, siis TTOS § 14 lg 1 p 3 kohaselt on töötaja kohustatud läbima tervisekontrolli vastavalt kehtestatud korrale. Siiski ei saa nende sätete alusel tööandja saata töötajat tervisekontrolli muudel põhjustel, näiteks joobe tuvastamiseks.¹⁴⁷

Vastavalt töötajate tervisekontrolli korra¹⁴⁸ § 5 lg-le 4 määrab töötervishoiuarst, olles tutvunud tervisekontrolli alusdokumentide ning töökohal töötaja töökeskkonna ja töökorraldusega, vajalikud terviseuuringud, kaasates vajadusel eriarste. Seega puudub tööandjal õigus kaasa rääkida, milliseid analüüse ja uuringuid töötajatele teha tuleb.

Tervisekontrolli läbiviival töötervishoiuarstil on tulenevalt TTOS § 19 lg 4 p-st 2 kohustus tagada töötajate tervise- ja eraeluandmete konfidentsiaalsus. Tööandjal on TTOS § 19 lg 4 p 3 alusel õigus saada tervisekontrolli tulemuste kohta teada ainult seda, millised piirangud on töötajale tööülesannete täitmiseks seatud tervise vastunäidustuste tõttu. Muid andmeid, näiteks töötaja analüüside tulemused, tööandjal töötaja tervisliku seisundi kohta õigus saada ei ole.

Seoses töötajate tervisekontrolliga võib tööandjale probleeme tekitada olukord, kui tööandja poolt tervisekontrolli suunatud töötaja keeldub sinna minemast. Põhjuseid selleks võib olla erinevaid, kuid üheks võimalikuks keeldumise põhjuseks võib olla töötaja usaldamatus tööandja poolt valitud töötervishoiuteenuse osutaja vastu. Kuna kõik tervist puudutav on inimeste jaoks väga isiklik ja delikaatne, siis reeglina inimesed valivad, kellega neid probleeme jagavad. Seda enam, et vastavalt töötajate tervisekontrolli korras esitatud töötaja tervisedeklaratsioonile peab töötaja töötervishoiuarstile avaldama ka sellised andmed, mis pole konkreetselt antud töö ohuteguritega seotud. Seega on mõisteta, miks töötaja võib soovida tervisekontrollist keelduda ning sellisel juhul töötaja sundimine töötervishoiuarsti vastuvõtule minema võib riivata töötaja õigust privaatsusele.

¹⁴⁷ Andmekaitse Inspeksioon, lk 46.

¹⁴⁸ Töötajate tervisekontrolli kord. SoMm 24.04.2003 nr 74. – RTL 2003, 56, 816.

Tööinspeksioon on seisukohal, et sellist kokkulepet töötaja ja tööandja omavahel sõlmida ei saa, millega töötaja kinnitab oma keeldumist tervisekontrollist ning võtab isikliku vastutuse töötervishoiu ja tööohutuse nõuete rikkumise eest.¹⁴⁹ Tervisekontrollist keeldudes ei riku TTOS-s ettenähtud kohustust ainult töötaja, vaid kui tööandja võimaldab töötajale seda, siis satub tööandja vastuollu TTOS § 12 lg-s 1 sätestatud nõudega tagada töötervishoiu ja tööohutuse nõuete täitmine igas tööga seotud olukorras.

Kuna kohustus läbida tervisekontroll tuleneb töötajale TTOS § 14 lg 1 p-st 3, siis tervisekontrollist keeldumine on töötajale seadusega kehtestatud kohustuse rikkumine. Vastavalt TLS § 88 lg 1 p-le 3 võib tööandja töölepingu erakorraliselt üles öelda, kui töötaja on hoiatusest hoolimata eiranud tööandja mõistlikke korraldusi või rikkunud töökohustusi. Seega peaks tööandja esmalt hoiatama töötajat ja juhtima tähelepanu tema kohustusele läbida ettenähtud tervisekontroll ning selgitama tervisekontrolli läbimata jätmise võimalikke tagajärgi (kutsehaigestumise riski suurenemine, töölepingu üles ütlemine tööandja poolt). Kui töötaja endiselt keeldub, siis on tööandjal õigus temaga tööleping lõpetada.

Samas ei ole töölepingu lõpetamine sellises olukorras alati lahenduseks, sest kui tegu on tööandja jaoks väärtusliku töötajaga, kes oma teisi töökohustusi täidab igati korrektselt, siis ei ole ilmselt kumbki töösuhte pool lepingu lõpetamisest huvitatud. Üheks võimalikuks lahenduseks oleks sellisel juhul see, et töötaja ja tööandja jõuavad kokkuleppele ja leitakse mõlemale poolele sobiv tervisekontrolli läbiviija. Muidugi saab tegu olla ainult erandliku olukorraga, sest on mõeldamatu, et tööandja hakkab igale töötajale vastavalt tema soovile töötervishoiuarsti otsima.

3.2 Kommunikatsioonivahendite kasutamise jälgimine

Tänapäeval toimub suur osa inimeste vahelisest suhtlusest kommunikatsioonivahendite kaudu, millest enimkasutatavad on kindlasti telefon, e-post, internetipõhised suhtlusportaalid (näiteks Facebook) ja -programmid (näiteks Skype, MSN). Seoses tehnika ja infotehnoloogia pideva arenguga sellise suhtlemise osakaal järjest suureneb, sest tehnika poolt vahendatud suhtluskanaleid tuleb pidevalt juurde. See puudutab nii töötajate erasuhtlust kui ka tööalast suhtlemist klientide ja koostööpartneritega.

¹⁴⁹ Tööinspeksiooni juhend – Töötaja omavastutus – kas lubada või mitte? Arvutivõrgus: [http://www.ti.ee/public/files/Tootaja%20omavastutus\(1\).pdf](http://www.ti.ee/public/files/Tootaja%20omavastutus(1).pdf), 22.01.2012.

Samas võimaldavad tänapäevased tehnilised lahendused ka seda, et töötajad lisaks oma tööülesannete täitmisele saavad töökohas tegeleda nõ isiklike asjadega, näiteks kirjutada ja lugeda isiklikke e-kirju, külastada oma kontot suhtlusportaalil, suhelda sõpradega Skype-i vahendusel. Kaasaegsed töötingimused on muutunud selliseks, et üha raskem on selgelt eristada töötunde eraelust, kuna järjest populaarsemaks on muutunud „kodukontor“ ning paljud töötajad jätkavad töötamist kodus, kasutades selleks tööandja poolt võimaldatud arvutisüsteeme.¹⁵⁰ See tingib omakorda selle, et töötajad ei pruugi alati hoida ranget vahet, et erasuhtluseks kasutatakse ainult isiklikke aadresse ja kontosid ning tööandja kommunikatsioonivahendid jäävad tööalaseks suhtlemiseks. Seda eriti olukorras, kus tööandja ja töötaja pole omavahel kokku leppinud, kas tööandja poolt tööülesannete täitmiseks töötaja kasutusse antud töövahendeid tohib töötaja kasutada ka eraotstarbeks ja kui tohib, siis millises ulatuses ning kas ja kuidas selle üle kontrolli teostatakse.

Probleemi ennetava lahendusena võib tööandja soovida piirata töötaja võimalusi kasutada tööandja poolt töötaja kasutusse antud töövahendeid mittetööalaseks kasutamiseks. Samas peab tööandja arvestama sellega, et kui tööandja on blokeerinud muude sidekanalite kasutamise võimaluse, siis peab ta võimaldama töötajal kasutada tööandja vahendeid.¹⁵¹

Tulenevalt eelnevast on tööandjal igati põhjendatud huvi kontrollida, kas töötaja kasutab tööaega efektiivselt ja tegeleb tööülesannetega või sisustab oma tööpäeva hoopis sõpradega suhtlemiseks. Samuti on õigustatud töötajate kommunikatsioonivahendite jälgimine tagamaks, et töötajad ei kasutaks tööandja sidevahendeid ebaseaduslikul eesmärgil.

Enne Eestis kehtiva korra analüüsimist võib võrdluseks välja tuua, et Suurbritannias on tööandjal äritegevuse eduka toimimise eesmärgil õigus jälgida töötaja tööalast elektroonilist sidet (telefonikõned, e-kirjad, faksid, internetiühendus) ilma töötaja nõusolekuta järgmistel juhtudel:

- tuvastamaks äritegevuse seisukohalt olulisi fakte;
- kontrollimaks vastavust asjakohastele protseduuridele ja praktikale;
- kontrollimaks töötajate saavutatud standardeid ja näitamaks, mida töötajad peaksid saavutama;
- kuritegude ennetamiseks või avastamiseks;

¹⁵⁰ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 6.

¹⁵¹ A. Jõks. Eraelu kaitse töösuhetes – väljakutse tööandjale. Ettekanne Andmekaitse inspeksiooni konverentsil.

- telekommunikatsiooni süsteemi lubamatu kasutamise avastamiseks või uurimiseks;
- süsteemi turvalisuse ja efektiivse toimimise tagamiseks.

Tööandjad peavad tegema kõik mõistlikud pingutused teavitamiseks sidevahendite kasutajaid, et nende tööalast suhtlust võidakse jälgida. Kui jälgimise käigus kogutakse, säilitatakse või kasutatakse isikuandmeid, peavad tööandjad järgima ka andmekaitse seaduses sätestatud nõudeid.¹⁵²

Soome legaliseeris 2009. aastal *Lex Nokia* nime all tuntud seadusemuudatusega elektrooniliste sidevahendite liiklusandmete jälgimise tööandja poolt. See muudatus annab tööandjale õiguse töödelda elektroonilise side liiklusandmeid ennetamiseks või uurimaks ärisaladuste avalikustamist ning sidevõrgu- või teenuse lubamatud kasutamist. Sellisest liiklusandmete töötlemisest tuleb eelnevalt teavitada andmekaitse ombudsmani. Töötajate sõnumite sisule see õigus ei laiene. Samuti puudutab see seadusemuudatus ainult elektroonilist sidet ning ei hõlma telefonisidet.¹⁵³

3.2.1 E-kirjad

Põhiliseks probleemide allikaks seoses e-kirjadega on see, et töötajad kipuvad kasutama tööandja poolt antud ning tööandja domeeni sisaldavat e-postiaadressi ka isiklikuks kirjavahetuseks. Selle on peamise probleemina tööandjate poolt AKI juhisele antud tagaside põhjal välja toonud ka Andmekaitse Inspeksioon.¹⁵⁴ Sageli teevad töötajad seda lihtsalt mugavusest, ilma põhjalikumalt kaalutlemata, kas neil on selleks õigus või kas see on ikka kõige parem lahendus. Kuna töö e-postiaadress on see, mida nad pidevalt jälgivad ja kasutavad, siis jõuavad sellele saadetud isiklikud kirjad tõenäoliselt kiiremini adressaadini ning samuti ei ole vaja kirjade lugemiseks ja saatmiseks täiendavalt kuhugi mujale kontole sisse logida. Tihti töötajad ilmselt ei teadvusta endale selle mugava lahendusega kaasnevat ohtu, et nii võivad isiklikud kirjad sattuda ka nende inimesteni, kellele need tegelikult mõeldud ei ole.

Töötajal ei ole mingit üldist õigust töö e-posti isiklikul eesmärgi kasutamiseks, kuid tööandjad peavad sellise väljakujunenud praktikaga ja sellest tuleneva töötaja õiguspärase ootusega

¹⁵² Information Commissioner's Office. The Employment Practices Code. Supplementary Guidance, 2005, lk 61–62. Arvutivõrgus: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/employment.aspx, 20.02.2012

¹⁵³ Act on the Protection of Privacy in Electronic Communications, section 13a, 13i.

¹⁵⁴ M. Filippov. Andmekaitse: tööalane ja erakirjavahetus olgu lahus. – Postimees 29.11.2011. Arvutivõrgus: <http://www.postimees.ee/651268/andmekaitse-tooalane-ja-erakirjavahetus-olgu-lahus/>, 27.02.2012.

privaatsusele arvestama seni, kuni nad pole ise kehtestanud teistsuguseid reegleid.¹⁵⁵ Seega, kui tööandja pole reegleid e-postiaadressi kasutamise kohta kehtestanud, peab ta arvestama sellega, et sinna võivad tulla ka töötaja isiklikud kirjad, mis kuuluvad sõnumisaladuse kaitsealasse. Kuna sõnumi saatmiseks kasutatud elektrooniliste seadmete asukoht ja nende kuulumine tööandjale ei välista põhiseaduses sätestatud õigust sõnumisaladusele.¹⁵⁶ Samuti fakt, et töötaja e-postiaadress kuulub tööandjale, ei tähenda seda, et tööandjale kuuluvad ka sealolevad e-kirjad, rääkimata sellest, et tööandja võiks neid lugeda.¹⁵⁷ Nagu eespool tõdetud sai, ei ole IKS-s sätestatud alused isikuandmete töötlemiseks kohaldatavad sõnumisaladuse riive õigustamiseks ja seega puudub tööandjal õigus piirata töötaja õigust sõnumisaladusele.

Sõnumisaladuse kaitsealasse kuuluvad vaid töötaja erakirjad – ja telefonikõned, kuna tööalased kirjad ja kõned teeb töötaja tööandja nimel ja huvides. Era- ja töökirjade eristamine võib kohati olla suhteliselt problemaatiline, sest isikliku kirjavahetuse hulka tuleb arvata ka töötajatevaheline kirjavahetus, mis ei seonu tööülesannete täitmisega.¹⁵⁸ See teeb eristamise veelgi keerulisemaks, kuna näiteks töökaaslastega vahetatud kirjad võivad sisaldada korraga nii tööalast informatsiooni kui ka eravestlust ning seetõttu ei saa tööandja ainult kirja saatja isikust lähtudes otsustada, kas tegu on töö- või erakirjaga. Seega peaks tööandja kasutusele võtma vastavad meetmed, mis aitaksid tööalaseid kirju erakirjadest eristada.

Kui töötaja erakirjad ei ole mingil moel eristatud või tähistatud ning tööandja poolt eraldatud domeeniga e-postiaadressi kasutamine eraotstarbel ei ole ka mitte mingil moel piiratud, on tõenäosus eraelu puutumatuse riiveks väga suur. Juba ainuüksi erakirjade saatmise-saamise kohta andmete vaatamine kujutab endast eraelu puutumatuse riivet. Kui tööandja ei ole kehtestanud ka mingeid reegleid selle kohta, kas ja kuidas toimub tööandja poolt töötaja e-postkastist info hankimine või töökohustuste rikkumiste menetlemine, ei erine töötaja õiguspärane ootus erasuhtluse privaatsusele tema muudest e-postkastidest.¹⁵⁹

Tegelikult ei ole kunagi võimalik täielikult välistada, et töötaja e-postkastis ei ole erasõnumeid. Seega ikkagi eksisteerib töötaja e-posti uurimisel oht riivata sõnumisaladust ja eraelu puutumatust. Selleks, et kontrollida mõnd töötaja tööalast kirja töötaja e-postkastist,

¹⁵⁵ Andmekaitse Inspeksioon, lk 57.

¹⁵⁶ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 20.

¹⁵⁷ N. Lugaresi. Electronic privacy in the workplace: Transparency and responsibility. – International review of Law, Computers & Technology 2010/24, No 2, lk 168.

¹⁵⁸ Andmekaitse Inspeksioon, lk 57.

¹⁵⁹ Andmekaitse Inspeksioon, lk 60.

tuleb rakendada meetmeid töötaja eraelu ja sõnumisaladuse riive vältimiseks. See, kas tööandja oma toiminguga riivab töötaja õigust sõnumisaladusele või eraelupuutumatusel või mõlemat korraga, sõltub igal konkreetsel juhul sellest, kas sõnum oli töötaja mõjusfääris. Selgelt saab töötaja mõjusfääris olevaks lugeda sellised e-kirjad, mille töötaja on avanud. Töötaja kontrolli all ei saa sõnum olla kuidagi siis, kui töötaja ei ole tööl ning tal puudub juurdepääs e-postkastile. Sõnum on jõudnud adressaadi mõjusfääri siis, kui see on laekunud tema postkasti ning tal on mõistlik võimalus sellega tutvuda.¹⁶⁰

Kui tööandjal peaks seoses töö korraldamisega tekkima möödapääsmatu vajadus ligi pääseda tööalasele informatsioonile, mis on tulnud töötaja postkasti e-kirjaga, aga töötajat ei ole tööl, siis peab tööandja selle teabe hankimiseks võtma kasutusele meetmed, millega kaasneb kõige väiksem oht töötaja põhiõigusi riivata. Kui siis tööandja kogemata leiab ja avab ka töötaja erakirja, peab selle vastavalt IKS § 24 p-le 1 viivitamata sulgema ning töötajat ja puudutatud kolmandat isikut teavitama. Erakirjaga seonduva info edasine töötlemine on keelatud. Andmekaitse Inspeksioon on seisukohal, et kui tööandja võttis töö korraldamiseks möödapääsmatult vajalikku info hankimisel tarvitusele kõik meetmed töötaja isikuandmete töötlemise vältimiseks, informeeris töötajat ning ei kasuta saadud isikuandmeid mingil muul eesmärgil, ei saa tööandjat süüdistada isikuandmete alusetu töötlemise eest.¹⁶¹

Kui töö korraldamise vajadusteks ei ole tööandjal töötaja erakirju vaja avada ega lugeda¹⁶², siis töötaja kontrollimise käigus võib tööandjal tekkida soov ka töötaja erakirju kontrollida – näiteks konkurentsikeelu ning konfidentsiaalsuskohustuse rikkumise tuvastamiseks. Kuna pigem võivad töökohustuste mittetäitmist tõendavad asjaolud ilmned just erasuhtluses, mis on sooritatud tööandja poolt tagatud sidevahendite kaudu.¹⁶³ Õigus sellisel juhul töötaja isikuandmeid töödelda (nii andmeid kirjade saatmise ja saamise kohta kui ka nende sisu kohta) on tööandjal vaid juhul, kui selline töötlemine tuleneb lepingust (IKS § 14 lg 1 p 4) või kui töötaja annab selleks nõusoleku. Kummalgi juhul ei tohi töötaja põhiõigusi ikkagi riivata ülemääraselt. Töötaja peab olema teadlik, et töötaja poolt saadetud ja vastuvõetud e-kirjad salvestatakse ning neid võidakse uurida töökohustuste rikkumise korral.¹⁶⁴ Seega on tööandja

¹⁶⁰ Andmekaitse Inspeksioon, lk 60, 62.

¹⁶¹ Andmekaitse Inspeksioon, lk 60–61.

¹⁶² Andmekaitse Inspeksioon, lk 60.

¹⁶³ A. Nõmper, K. Michelson. Kas tööandja saab sidevahendite kasutamist kontrollida? Arvutivõrgus: <http://www.e24.ee/240487/kas-tooandja-saab-sidevahendite-kasutamist-kontrollida/>, 19.02.2011

¹⁶⁴ Andmekaitse Inspeksioon, lk 63.

jaoks siiski ainuke efektiivne kaitsevahend kokkulepe, milles fikseeritakse töötajaga ühiselt infotehnoloogiliste vahendite sihtotstarbelise kasutamise jälgimine.¹⁶⁵

Kui tööandja on saadetud ja vastuvõetud e-kirjade salvestamisel seadnud eesmärgiks ainult tööalase kirjavahetuse säilitamise, ei või tööandja IKS § 6 punktides 2 ja 4 sätestatud eesmärgikohasuse põhimõttest ja kasutuse piiramise põhimõttest tulenevalt uurida töötaja e-postkastis olevaid erakirju.¹⁶⁶

Samas peab tööandja arvestama, et töötaja erakirjade uurimine võib rikkuda ka kolmandate isikute (erakirja saatjate ja saajate ning muude isikute, keda kirjades nimetatakse) eraelu puutumatust kui ka nende sõnumisaladust. IKS § 14 lg 1 p 4 ega töötaja nõusolek ei anna tööandjale alust töödelda kolmandate isikute isikuandmeid, kuna töötaja ja tööandja ei saa omavahel kokku leppida kolmandate isikute õiguste üle. IKS-i kohaselt saaks kolmandate isikute andmete töötlemise aluseks olla sellises olukorras kolmanda isiku nõusolek. AndmekaitseDirektiivi artikkel 7 punkti f kohaselt oleks kolmandate isikute isikuandmete töötlemine lubatud tingimusel, et see on vajalik tööandja õigustatud huvide elluviimiseks ning selliseid huve ei kaalu üles andmesubjekti põhiõigused ja – vabadused. Seega andmekaitseDirektiivi silmas pidades peaks igas niisuguses olukorras hindama tööandja konkreetsete huvide olulisust – kas need ikka õigustavad sekkumist kolmandate isikute põhiõigustesse.¹⁶⁷

Soomes on seadusega väga täpselt reguleeritud, millistel juhtudel ja tingimustel on tööandjal õigus töötaja e-postkastist kirju otsida ja neid avada. Tööandjal on õigus otsida ja avada e-kirju, mis on saadetud tööandja poolt töötajale eraldatud meiliaadressile või mis on sellelt aadressilt töötaja poolt saadetud, ainult juhul, kui tööandja on võtnud kasutusele vajalikud abinõud kaitsmaks töötajale ning töötaja poolt saadetud e-kirju. Selleks peab tööandja tagama, et töötajal oleks võimalik automaatvastuse funktsiooni abil edastada e-kirja saatjale automaatne teade töötaja eemaloleku ja selle kestvuse kohta ning selle kohta, kes töötajat sel ajal asendab. Alternatiivina on töötajal võimalus suunata e-kirjad tööandja nõusolekul teisele isikule või aadressile või töötaja saab anda nõusoleku selleks, et tema äraoleku ajal keegi teine vaatab tema e-kirju eesmärgiga tuvastada, kas töötajale saadetud kirjad on selgelt tööalase sisuga ning selles sisalduv informatsioon on tööandjale töö korraldamiseks oluline. Lisaks on seadusega sätestatud veel konkreetsed eeldused, mis peavad olema täidetud tööandja poolt

¹⁶⁵ A. Nõmper, K. Michelson. Kas tööandja saab sidevahendite kasutamist kontrollida?

¹⁶⁶ Andmekaitse Inspeksioon, lk 63.

¹⁶⁷ Andmekaitse Inspeksioon, lk 63.

töötaja e-kirja otsimiseks või avamiseks. Samuti tuleb nii kirjade otsimise kui ka avamise kohta koostada raport, milles kajastatakse kirjade otsimise või avamise põhjus, aeg, läbiviijad ning kirja avamise korral märgitakse ära ka konkreetne kiri, mida avati ja see, kellele kirjas sisalduv informatsioon edastati. Selle raporti allkirjastavad kõik asjaosalised. Raport esitakse töötajale ilma põhjendamatu viivitusega.¹⁶⁸

Kuivõrd tööandjal on kontroll töötaja e-postkasti üle, peab tööandja IKS §-st 25 tulenevalt võtma tarvitusele meetmed õigustamata isikute juurdepääsu takistamiseks sellele, kaitsmaks nii töötajate kui ka e-kirjades sisalduvate kolmandate isikute andmeid. Selleks peab tööandja rakendama isikuandmete töötlemiseks sobivaid organisatsioonilisi, füüsilisi ja infotehnoloogilisi turvameetmeid.¹⁶⁹ Tööandja peab tagama, et kõik arvutid ja postkastid oleksid varustatud vajalike paroolidega, et nii võõrastel isikutel kui ka kaastöötajatel, kel see tööülesannete tõttu vajalik ei ole, puuduks nendele ligipääs. Samuti tuleb töötajaid turvanõuetest teavitada ja nõuda töötajatelt nende järgimist. Lisaks peaks tööandja kaitsma töötajate e-postiaadresse spämmifiltridega, et vähendada töötaja postkasti tulevaid rämpskirju. Kuna saades tööandja meilisüsteemi vahendusel pealesunnitud e-kirju kolmandatelt isikutelt (spämmi), rikub see töötaja õigust olla rahule jäetud (*right to be let alone*).¹⁷⁰

3.2.2 Internet

Kõige lihtsam moodus lahendada töötaja interneti kasutamisega seotud probleemid, oleks ilmselt see, kui töötaja tööarvutis puuduks täielikult juurdepääs internetile. Paraku oleks see mõeldav ainult sellises olukorras, kus töötaja oma tööülesannete täitmiseks üldse internetti ei vaja. Kuna interneti kasutamine on tänapäeval muutunud nii elementaarseks, siis arvutiga töötajad peavad reeglina ka oma tööülesannete täitmiseks vähemal või suuremal määral internetti kasutama ning selline piirang hakkaks segama ka tööd ja seega enamikel juhtudel ei oleks mõeldav. Samas ei ole ilmselt ka enamuse tööandjatel selle vastu midagi, kui töötajad tööarvutis mõne isikliku toiminguga teevad, kui nad teevad seda mõistlikus mahus ning see ei sega nende tööd. Näiteks lõunapausi ajal maksavad internetipangas oma arveid, esitavad elektrinäite või käivad isiklikku e-postkasti vaatamas.

¹⁶⁸ Act on the Protection of Privacy in Working Life, section 18, 19, 20.

¹⁶⁹ Andmekaitse Inspektsioon, lk 58.

¹⁷⁰ N. Lugaresi, lk 170.

Euroopa andmekaitseasutuste tööühm on arvamisel, et isiklikul otstarbel interneti kasutamise täielik keelustamine on ebapraktiline ja veidi ebareaalne, kuna see ei kajasta seda, mil määral internet töötajaid nende igapäevaelus abistab. Sealsamas on aga tööühm märkinud, et see on ettevõtte otsustada, kas ja millises ulatuses on töötajatel lubatud internetti eraotstarbel kasutada.¹⁷¹ Seega ei ole töötajal mingit üldist õigust kasutada tööl olles internetti oma isiklikuks otstarbeks ning selle lubamine või keelamine sõltub tööandjast.

Kui tööandja on töötajatele võimaldanud vaba juurdepääsu internetile, siis ei tähenda see seda, et tööandjale ei oleks põhjust ega õigust töötajate internetikasutust jälgida. Kuigi kõikehõlmav ja piiramatu jälgimine tööandja poolt on välistatud, siis mõõdukas jälgimine on tööandjale vajalik kontrollimaks äritegevuse toimimist. Samuti on väga lihtne interneti kasutust kuritarvitada. Internet on oma olemuselt neutraalne ning töötajad võivad sealt otsida kõike, aga ilma tõhusa kontrollita on palju võimalusi interneti ebasobivaks ja isegi kriminaalseks kasutamiseks.¹⁷²

Sellest tulenevalt võib tööandja soovida kontrollida töötaja internetikasutust eelkõige selleks, et veenduda, kas töötaja täidab tööajal ikka oma töökohustusi või veedab aega hoopis tööga mitteseotud internetilehekülgedel. Samas on tänapäeval internetist saanud üks põhilisemaid infoallikaid, mida töötaja võib kasutada ka oma tööülesannete täitmiseks ning seetõttu ainult töötaja internetis viibimise aja järgi ei saa kindlaks teha, kas töötaja kasutab oma tööaega efektiivselt või mitte. Seega, saamaks vastust sellele küsimusele, peaks tööandja uurima täpsemalt lehekülgi, mida töötaja on külastanud, mis aga omakorda on tunduvalt suurem töötaja privaatsuse riive kui lihtsalt internetis viibitud aja jälgimine. Kuid ka see meede ei pruugi anda selget ülevaadet, kuna kindlasti on selliseid lehekülgi, mida töötaja võib kasutada nii töö- kui eraasjade ajamiseks. Näiteks töötaja, kelle ülesandeks on ettevõttes ärireiside korraldamine, võib reisibüroo kodulehel olla nii tööasjus, kuid samas võib ta ka planeerida seal oma puhkusereisi. Seega ei pruugi internetikasutamise andmete jälgimine anda alati adekvaatset infot ning kui meede oma eesmärgi ei täida, siis ei ole ka töötaja privaatsusesse sekkumine õigustatud.

Vältimaks töötaja põhiõiguste ülemäärast riivet, tuleks enne töötaja internetikasutuse jälgimist väga hoolikalt kaaluda, kas selline jälgimine annab adekvaatset infot töötaja töökohustuste

¹⁷¹ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 24.

¹⁷² N. Lugaresi, lk 165.

täitmise kohta. Kui töötaja tööd on võimalik hinnata töö tulemuste alusel, ei pruugi töötaja internetikasutuse jälgimine olla üldse põhjendatud.¹⁷³

Tööandja võib soovida töötaja internetikasutust jälgida ka turvalisuse kaalutlusel, et töötajad ei käiks kahtlastel ja keelatud internetilehekülgedel, ega laadiks sealt alla kogu ettevõtte arvutisüsteemi ohustavaid arvutiviiruseid või tegeleks mu illegaalse tegevusega. Ka sellisel juhul töötaja internetikasutamise jälgimine ei ole kõige õigem meede probleemi lahendamiseks, kuna sel hetkel, kui tuvastatakse, et töötaja on käinud keelatud leheküljel, võib olla arvutisüsteem juba kahjustatud. Arvutisüsteemide turvalisust aitavad pigem tagada ennetavad meetodid, nagu näiteks keelata teatud lehekülgedele juurdepääs ning piirata töötajate arvutite kasutajaõigusi selliselt, et lisaprogrammide installeerimine oleks võimatu. Ennetamine on palju olulisem ja tõhusam kui rikkumiste avastamine ehk tööandja huvid on paremini kaitstud ennetades spetsiaalsete tehniliste vahendite abil internetikasutuse kuritarvitamist, kui kulutades vahendeid rikkumiste tuvastamisele.¹⁷⁴ Andmekaitse Inspektsiooni hinnangul on äärmiselt kaheldav, et töötaja internetikasutuse analüüsimine on kõige kohasem vahend turvalisuse tagamiseks.¹⁷⁵

Tööandja võib huvi tunda ka selle vastu, mida töötaja on interneti üles pannud. Tööandja huvi võib olla põhjendatud näiteks sellega, et tööandja tahab olla kindel, et tema töötajad oma arvamuste ja kommentaaridega ei kahjustaks tööandja mainet. Kui tööandja uurib, mida töötaja on eraviisiliselt interneti üles riputanud, siis ka see on käsitletav isikuandmete töötlemisena. See riivab töötaja õigust väljendusvabadusele, kuna seab piirangu töötaja arvamuse avaldamisele internetis, sest kartes tööandjapoolset reaktsiooni ja tagajärgi avaldatud kommentaaridele, ei pruugi töötaja julgeda oma arvamust avameelselt avaldada.

Kui tööandja ikkagi soovib töötaja internetikasutust jälgida, siis olenemata sellest, millisel viisil töötajate internetikasutust jälgitakse, peab tööandja sellest töötajaid teavitama. Tööandja peab arvestama, et internetikasutuse andmed võivad avaldada töötaja kohta väga suures ulatuses eraelulist informatsiooni, sh viiteid delikaatsetele isikuandmetele, mistõttu riive töötaja eraelule võib olla väga ulatuslik. Seega peavad internetikasutuse uurimise eesmärgid olema sõnastatud selgelt ja üheselt mõistetavalt. Ei piisa sellest, kui eesmärgina nimetatakse „töötaja kontrollimist“ või „töökohustuste kontrollimist“, vaid tuleks täpsustada, milliste

¹⁷³ Andmekaitse Inspektsioon, lk 65–66.

¹⁷⁴ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 24.

¹⁷⁵ Andmekaitse Inspektsioon, lk 65.

töökohustuste kontrollimiseks peab tööandja vajalikuks töötajate internetikasutuse andmeid uurida.¹⁷⁶

Lisaks internetikasutuse jälgimise eesmärkidele tuleks töötajaid informeerida ka jälgimise meetmetest ning sellest, kuidas töötajaid rikkumisest teavitatakse. Kui tööandja töötaja internetikasutuse jälgimisel avastab töötaja rikkumise, siis on soovitatav sellest töötajat viivitamatult teavitada. Elektrooniliste kommunikatsioonivahendite puhul saab selleks kasutada automaatteateid, mis ilmuvad ekraanile ja hoiatavad töötajat, et arvutisüsteem on avastanud lubamatu internetikasutuse.¹⁷⁷

Internetikasutuse jälgimise meetodit valides peab tööandja arvestama TLS § 28 lg 2 p-ga 11 ning sellest tulenevalt austama töötajate privaatsust ning teostama kontrollimist viisil, mis ei riiva ülemääraselt töötajate põhiõigusi. Enamlevinud on töötajate internetikasutuse jälgimine läbi infotehnoloogiliste vahendite, kuid seda on võimalik teha ka ruumi paigutatud kaamera kaudu. Sellisel juhul peab tööandja arvestama ka käesoleva töö alapeatükis 3.3 käsitletut.

Töötaja internetikasutuse jälgimisel kogutud andmeid peaks tööandja säilitama ainult seni, kuni see on vajalik jälgimistegevuse eesmärgi saavutamiseks.¹⁷⁸ Seega ei ole põhjendatud, et tööandja säilitaks töötajate internetikülastuste ajalugu kindlaks määramata perioodi jooksul. Andmete säilitamise periood 1-2 kuud peaks olema üldjuhul töötaja rikkumise tuvastamiseks piisav.

3.2.3 Telefon

Töötaja telefoni kasutamise jälgimise ja kontrollimisega kaasnev töötaja privaatsuse riive oht on kõige suurem kindlasti töötaja telefonikõnede salvestamise korral. Nii nagu kodus tehtud telefonikõned, kuuluvad ka töökohal tehtud telefonikõned eraelu puutumatuse ja sõnumisaladuse kaitsealasse.¹⁷⁹ Telefonikõne sisu on selle toimumise ajal sõnumisaladuse kaitsealas. Samas eeldusel, et tegemist on tõepoolsest töökõnedega, ei kuulu need töötaja personaalse sõnumisaladuse ega ka eraelu puutumatuse kaitsealasse. Küll aga tuleb arvestada,

¹⁷⁶ Andmekaitse Inspektsioon, lk 65.

¹⁷⁷ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 15.

¹⁷⁸ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 14.

¹⁷⁹ EIKo 25.06.1997, 20605/92, *Halford vs. Ühendkuningriik*.

et kõne on kaitstud kõne teiseks pooleks oleva isiku sõnumisaladusega. Kui lindistamise õigus ei tulene seadusest, peab kõne teist poolt lindistamisest hiljemalt kõne alguses selgelt teavitama ning IKS § 10 lg 1 kohaselt peab olema andmete töötlemiseks isiku nõusolek.¹⁸⁰

Selleks, et pakkuda klientidele heal tasemel klienditeenindust, on levinud klienditeeninduse telefonikõnede salvestamine. Samas tuleks kaaluda, kas on vajalik kõigi telefonikõnede salvestamine või annaks sama tulemuse ka pisteline kõnede salvestamine või ainult nende klienditeenindajate kõnede salvestamine, kelle kohta on esitatud tööandjale kaebusi. Selline valikuline salvestamine riivaks nii töötajate kui ka klientide privaatsust tunduvalt vähem.

Andmekaitse Inspeksioon soovib samuti analüüsida, kas kõikide kõnede salvestamise meede on tõepoolest nii efektiivne ning kas sellele meetmele pole muid alternatiive – eriti delikaatseid isikuandmeid sisaldavate kõnede lindistamise puhul ei pruugi meetmega saavutatav kasu kaaluda üles kolmandate isikutele kaasnevat ebamugavust, teadmatust ning hirmu.¹⁸¹

Töötaja eraviisilised kõned on kaitstud töötaja ja kõne teise poole sõnumisaladusega. Seega, kui töötajad võivad töötelefoni kasutada ka isiklikuks otstarbeks, peaks töötajal olema võimalus erakõnede ajal salvestamine peatada või salvestis ise viivitamatult jäädavalt kustuda.¹⁸²

Üsna levinud on töötaja poolt tehtud telefonikõnede andmete töötlemine sellisel juhul, kui töötajal on küll lubatud töötelefoni kasutada ka erakõnedeks, kuid tehtud erakõned peab töötaja hiljem tööandjale hüvitama. Sellisel juhul ei töödelda telefonikõnede sisu, vaid nn telefonikõne liiklusandmeid (valitud telefoninumbreid, kõne kestvus ja toimumise aeg), mis kuuluvad töötaja eraelu puutumatuse kaitsealasse. Ainuüksi asjaolu, et tööandja seaduslikult omandab selliseid andmeid telefoniarve kujul, ei välista sekkumist töötaja õigusesse eraelu puutumatusele.¹⁸³

Kui töölepingus on kokku lepitud töötaja õigus kasutada tööandja poolt antud telefoni ka erakõnedeks, ei tähenda see, et tööandja võiks vabalt uurida töötaja poolt tehtud kõnede andmeid. Näiteks, kui kokkuleppe kohaselt hüvitab telefoniarve limiiti ületava summa töötaja,

¹⁸⁰ Andmekaitse Inspeksioon, lk 64.

¹⁸¹ Andmekaitse Inspeksioon, lk 64.

¹⁸² Andmekaitse Inspeksioon, lk 65.

¹⁸³ EIKo 09.04.2007, 62617/00, *Copland vs. Ühendkuningriik*.

ei ole tööandjal üldse mingit põhjust uurida, mis asjaoludel limiiti ületati. Kui lepingu kohaselt hüvitab töötaja tööandjale erakõnede maksumuse, peaks Andmekaitse Inspektsiooni hinnangul töötaja ise esitama andmed selle kohta, millise summa eest ta erakõnesid tegi. Samas on Andmekaitse Inspektsiooni hinnangul iga arve puhul ülemäärane nõuda, et töötaja märgiks kõneeristuses ära erakõned. Kui tööandjal on tõepoolest põhjendatud kahtlus töötaja poolt erakõnede maksumuse kohta esitatud andmete tõele vastavuses, peaks tööandja piirduma sellega, et uurib kõneeristuses valitud numbrite esinemissagedust ja/või kõnede kestvust ning nõuab seejärel töötajalt selgitusi selliste kõnede asjaolude kohta. Vältimaks kolmandate isikute isikuandmete töötlemist, ei tohiks tööandja hakata ise internetist või telefoniraamatust uurima, kellele kuuluvad telefoninumbrid, millele on töötaja helistanud. Samuti ei ole reeglina üldse vaja uurida sissetulevaid kõnesid.¹⁸⁴

3.2.4 Kommunikatsioonivahendite kasutamise reeglid

Tuginedes eespool toodule, oleks nii töötaja kui ka tööandja enda huvides tööandjal mõistlik kehtestada töötajatele konkreetsed ja üheselt mõistetavad reeglid tööandja poolt töötajale tööülesannete täitmiseks eraldatud sidevahendite kasutamiseks, tuues nendes eeskirjades selgelt välja ka nende kommunikatsioonivahendite jälgimise fakti ja selle läbiviimise korra. Kui tööandja pole selliseid reegleid kehtestanud ja neid töötajatele tutvustanud, siis töötajal on õiguspärane ootus privaatsusele ja ta võib eeldada, et mingit jälgimist ei toimu.¹⁸⁵ Need reeglid võib kehtestada eraldi dokumendina, kuid otstarbekam oleks, kui need eeskirjad moodustaksid ühe osa ettevõtte töökorralduse reeglitest või privaatsuspoliitikast. Lähtudes AKI juhiseist¹⁸⁶, Euroopa andmekaitseasutuste töörühma soovituselt¹⁸⁷ ning UK juhiseist¹⁸⁸, võiks välja tuua järgmise näidisloetelu punktidest, mida tööandja nende reeglitega kehtestada võiks:

- Esmalt peaks tööandja selgelt ja üheselt mõistetavalt välja tooma, kas töötajad võivad tööandja sidevahendeid kasutada ka erasuhtluseks ja kui see on lubatud, siis millistel tingimustel ning mahus töötajad seda teha tohivad. Näiteks võib tööandja kehtestada isiklikele telefonikõnede rahalise või ajalise limiidi või keelata isiklikud rahvusvahelised kõned;

¹⁸⁴ Andmekaitse Inspektsioon, lk 64.

¹⁸⁵ N. Lugaresi, lk 167.

¹⁸⁶ Andmekaitse Inspektsioon, lk 58–61.

¹⁸⁷ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 22.

¹⁸⁸ Information Commissioner's Office. The Employment Practices Code, lk 69–70.

- Kui tööandja on lubanud kasutada kommunikatsioonivahendeid isiklikuks otstarbeks, siis tuleks kehtestada selged reeglid selle kohta, kas neid võib kasutada ka väljaspool töökohta ja tööaega (näiteks sülearvutid, mobiiltelefonid);
- Eeskirjades tuleb täpselt määratleda töötaja kommunikatsioonivahendite kasutamise jälgimise eesmärgid, meetodid ja ulatus. Samuti selgelt sõnastada kehtestatud reeglite rikkumise võimalikud tagajärjed;
- Kui tööandja soovib töötajate internetikasutust piirata, tuleks täpsustada, milliste lehtede külastamine on keelatud. Näiteks on keelatud tasuliste ning pornograafilise sisuga internetilehekülgede külastamine, piraattarkvara pakkuvate lehtede külastamine ning sealt tarkvara allalaadimine;
- Tööandja võib kehtestada nõude, et tööandja domeeniga e-postiaadressi ei või töötajad kasutada isiklike e-kirjade saatmiseks. Samas ei välista see, et sinna postkasti ei saadetak töötajale erakirju kolmandate isikute poolt. Siiski võib tööandja sellise reegli kehtestamise korral eeldada, et töötaja poolt saadetud kirjad on tööalased kirjad;
- Kui tööandja lubab töötajal kasutada töö e-posti ka erasuhtluseks, võiks olla kehtestatud reegel, et erakirjad tuleb postkastist kustutada või tõsta spetsiaalselt loodud alamkausta, mis oleks selgelt eristatud näiteks pealkirjaga „Isiklik“. Alternatiivselt võiks erakirjade pealkirjad tähistada sellisel viisil, et tööandjal oleks võimalik juba pealkirja järgi aru saada, et tegemist on erakirjavahetusega. Sellise reegli kehtestamisel võib tööandja eeldada, et töötaja poolt saadetud ilma „isikliku“ märketa üldises kaustas olevad kirjad on tööalased kirjad;
- Töötaja postkastist info otsimise vältimiseks võib tööandja kehtestada nõude, et e-kirjades olev tööalaselt vajalik info salvestatakse ka tööandjale või teistele töötajatele juurdepääsetavale andmekandjale;
- Kontorist eemaloleku ajaks peaksid töötajad rakendama kontorist väljasoleku automaatvastust, mille reeglina lülitaksid sisse töötajad ise, kuid erakorralistel juhtudel peaks see õigus olema ka tööandjal või mõnel selleks töötaja poolt määratud kaastöötajal;

- Töötaja töölt eemaloleku ajaks võib ette näha e-kirjade automaatse edasi suunamise töötajat asendavale või töötaja enda poolt määratud teisele töötajale;
- Töötaja võib kokkuleppel tööandjaga määrata kindlaks teise töötaja, kellel on õigus töötaja e-postkasti tema äraolekul avada;
- Kirja saajate teavitamiseks võib väljasaadetavatele kirjadele juurde lisada märkuse, et tegemist on ettevõtte tööalase e-postiaadressiga, millele saadetavat informatsiooni töödeldakse ettevõttes vastavalt kehtestatud sisekorraeeskirjadele. Kirja saajat aitab teavitada ka kirja alla lisatav standardiseeritud infolõik ettevõtte nime, kontaktandmete ning kirja saatja ametikoha kohta;
- Täpsustada tuleks töösuhte lõppemise korral töötaja poolt tööga seotud dokumentatsiooni üleandmise nõuet selliselt, et see selgelt hõlmaks ka töötaja e-postkastis olevaid tööalaseid kirju. Tööandjal ei ole töötaja e-postkasti avatuna hoidmiseks peale töösuhete lõppu otsest seadusest tulenevalt alust, kuid see võib olla reguleeritud töölepingus või annab töötaja selleks nõusoleku. Kui e-postkasti avatuna hoidmise võimalust pole töölepinguga reguleeritud ning lahkuv töötaja nõusolekut ei anna, tuleb postkast koheselt peale töösuhte lõppemist sulgeda. Vastasel juhul töödeldakse töötaja ja potentsiaalselt ka kolmandate isiku isikuandmeid ilma õigusliku aluseta (näiteks e-postiaadress sisaldab töötaja nime, keegi saadab selle aadressile isikliku kirja);
- Lisaks tuleks reguleerida ka töötajale eraldatud e-postkastiga seotud tööandja enda õigused ning lisada infosüsteemi administraatorite jt töötaja e-postile juurdepääsu omavate isikute töölepingusse konfidentsiaalsuskohustus. Tööandja poolt töötajale eraldatud e-postkastist info hankimine tuleks täpselt reguleerida, millistel asjaoludel seda teha tohib, kes toimingut teeb, kuidas toiming tehakse, millal toiming tehakse ja kuidas töötajat sellest teavitatakse;
- Veel võiks tööandja nendes reeglites reguleerida selle, kas ja kuidas tehakse e-kirjadest varukoopiaid ning kui pikalt neid koopiaid säilitatakse. Samuti selle, kas ja millal e-kirjad serverist lõplikult kustutakse;

Reegleid koostades peab tööandja selgelt määratlema andmete töötlemise eesmärgid, kontrollima valitud meetme proportsionaalsust ja lähtuma minimaalsuse ning läbipaistvuse

nõudest. Lisaks peab tööandja arvestama, et eeskirjadega ei saa tööandja kehtestada selliseid piiranguid ega luua endale õigusi, mis on vastuolus põhiseaduse või teiste seadustega. Eeskirjade kehtestamine ei vabasta tööandjat IKS-s sätestatud kohustuste täitmisest ega võimalikust vastutusest ebaseadusliku tegevuse eest.¹⁸⁹ Eelnev hoiatamine ei ole piisav, et õigustada töötajate isikuandmete kaitse rikkumisi.¹⁹⁰

Reeglite kehtestamisest üksi ei piisa, tööandja peab tagama ka selle, et töötajad oleksid nendest kehtestatud eeskirjadest teadlikud. Loomulikult tuleb neid reegleid tutvustada töötajatele tööleasumisel ning tööandja poolt reeglite muutmisel. Samas võiks meeldetuletus reeglite olemasolust ja nende järgmise kohustustest ilmuda automaatselt töötaja arvutiekraanile igakordsel arvuti sisselülitamisel.

3.3 Jälgimisseadmete kasutamine

Turvaseaduse¹⁹¹ § 11 lg 3 kohaselt on jälgimisseadmestik pilti või elektroonilist signaali edastavate ja salvestavate seadmete kogum, mis on ette nähtud territooriumi, inimese, eseme või protsessi jälgimiseks või territooriumi, inimese või eseme asukoha või protsessi toimumise koha kindlaksmääramiseks. Seega on jälgimisseadmeteks tööandja poolt kasutatavad turva- ja videokaamerad kui ka sõidukisse paigaldatavad GPS – seadmed. Samuti võib siia hulka arvata uksekaardisüsteemid, mis võimaldavad jälgida töötajate liikumist ettevõtte ruumides.

Jälgimisseadmete kasutamine kujutab endast, võrreldes teiste isikuandmete kogumise viisidega, kõige intensiivsemat eraelu riivet üldse. Läbimõeldamatu jälgimisseadmete kasutamine võib tööandjale kokkuvõttes tuua rohkem kahju kui kasu – seda eeskätt usaldamatuse õhkkonna loomise, stressi põhjustamise aga ka töötajate inimväärikuse alandamise kaudu.¹⁹²

Seega tuleb tööandjal enne jälgimisseadmete kasutusele võtmist iga konkreetse juhtumi korral hoolikalt kaaluda ühelt poolt selle meetme kasulikkust ja vajalikkust ning teiselt poolt sellega kaasneda võivat töötajate ja kolmandate isikute privaatsusõiguse riivet. Kas saavutatav

¹⁸⁹ Andmekaitse Inspeksioon, lk 59.

¹⁹⁰ Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, lk 9.

¹⁹¹ Turvaseadus. – RT I 2003, 68, 461 ... RT I, 29.12.2011, 51.

¹⁹² Andmekaitse Inspeksioon, lk 66.

eesmärk ikka õigustab teiste isikute privaatsusesse sekkumist ning ega valitud meede ei too kaasa isikuandmete ülemäära töötlemist. Selle olukorra hindamiseks tuleks kaaluda järgmisi asjaolusid:

- Mis on jälgimisseadme kasutamisest saadav kasu ja kas see kaalub üle sellega kaasnevad kahjulikud mõjud?
- Kas jälgimissüsteemi eesmärk on selgelt määratletud, üheselt mõistetav ja õigustatud? Kas videojälgimisele on seaduslik alus?
- Kas jälgimisseadme kasutamine on ilmselgelt vajalik? Kas see on efektne meede soovitud eesmärgi saavutamiseks ning ega pole olemas põhiõigusi vähem riivavaid alternatiive?¹⁹³

Jälgimisseadmete kasutamist ei saa õigustada üldise viitega võimalikele rikkumistele, mis ettevõtte territooriumil võivad aset leida. Iga turvarisk tuleks määratleda eraldi ja detailselt, tuginedes reaalselt ja tõestatavatele andmetele riski olemasolu ja ulatuse kohta. Pelk hirm, spekulatsioon või naeruväärne tõendus ei ole piisavad, et õigustada jälgimisseadmete kasutamist. Lisaks tuleks määratleda, kas jälgimisseadmete kasutamise eesmärk on konkreetse turvariski ennetamine või uurimine.¹⁹⁴

Jälgimisseadmeid kasutades peab tööandja arvestama, et kui isik on jälgimisseadmete abil tuvastatav, leiab isikuandmete töötlemine aset sõltumata sellest, kas jälgimisseadme salvestusi vaadatakse läbi või mitte. Identifitseeritav on isik ka siis, kui jälgimisseadmete abil pildilt ei nähtu tema nägu, kuid isikut on võimalik identifitseerida tema muude tunnuste kaudu, näiteks keha kuju, riietus, kaasas olevad asjad.¹⁹⁵

Jälgimisseadmete abil võib isikuandmeid töödelda isiku nõusolekul, lepingu täitmiseks või seaduse alusel. Kuid IKS § 14 lg 3 sätestab siinkohal erandi, mil isiku nõusolekut vaja ei ole - isikute või vara kaitseks võib isikuandmeid edastavat või salvestavat jälgimisseadmestikku kasutada, kui sellega ei kahjustata ülemääraselt andmesubjekti õigustatud huve ning kogutavaid andmeid kasutatakse ainult nende kogumise eesmärgist lähtuvalt. Andmesubjekti nõusolekut asendab sellise andmetöötlemise korral jälgimisseadmestiku kasutamise fakti ning andmete töötleja nime ja kontaktandmete piisavalt selge teatavakstegemine.

¹⁹³ European Data Protection Supervisor. Video-surveillance Guidelines, 2010, lk 16–17. Arvutivõrgus: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf, 01.02.2012.

¹⁹⁴ European Data Protection Supervisor. Video-surveillance Guidelines, lk 20.

¹⁹⁵ Andmekaitse Inspeksioon, lk 66–67.

Samas ei saa seda erandit kohaldada töötajate kontrollimise eesmärgil töötajate jälgimisele. Seega tuleb jälgimisseadmeid, mida kasutatakse klientide, hoonete ja seadmete jälgimiseks isikute või vara kaitseks, eristada neist seadmetest, mis on suunatud konkreetsetelt töötajate tegevuse jälgimisele.¹⁹⁶ Samuti kui jälgimissüsteem on paigaldatud turvalisuse eesmärgidel ja ka töötajaid on ainult sellest eesmärgist teavitatud, siis ei saa jälgimisseadme salvestusi kasutada kontrollimaks, kuidas töötajad täidavad oma tööülesandeid või kas nad tulevad õigel ajal tööle.¹⁹⁷

Kui tööandja soovib töötajate kontrollimiseks kasutada jälgimisseadmeid, peab ta iga konkreetse juhtumi korral hindama, kas töötajate jälgimine on põhjendatud ja lubatud ning kui on, siis milline oleks mõlema poole huve arvestades kõige mõistlikum viis selle läbi viimiseks. Igasugune töötajate jälgimine peab olema proportsionaalne meede nende riskide suhtes, mis tööandjal on ning seejuures peab tööandja arvestama töötajate privaatsuse ja muude huvidega. Igasugused isikuandmed, mida jälgimise käigus kogutakse või töödeldakse, peavad olema adekvaatsed, asjakohased ja mitte ületama jälgimise eesmäärke. Jälgimist tuleb teostada võimalikest leebemal viisil.¹⁹⁸ Samuti peaks vältima töötajate pidevat jälgimist, seega ei tohiks töötajad olla pidevalt turvakaamera vaateväljas.¹⁹⁹

Euroopa andmekaitseasutuste tööühm on arvamisel, et distantilt töötaja jälgimine tema töö kvaliteedi ja hulga kontrollimise eesmärgil ei ole lubatav. Aktsepteeritav on jälgimisseadmete kasutamine näiteks tööprotsesside ja tööohutuse tagamise vajadusteks, kuid sellisel juhul peaks eelnevalt konsulteerima töötajate usaldusisiku või ametiühinguga jälgimise täpsete asjaolude suhtes.²⁰⁰

Euroopa Andmekaitseinspektor on seisukohal, et ainuüksi kvaliteedikontroll, ettevõtte poliitikate juurutamine või vaidluste puhuks tõendite tagamine ei ole piisavad õigustused jälgimissüsteemi rakendamiseks. Sisejuurdluseks on jälgimisseadmete kasutamine võimalik vaid juhul, kui tegemist on füüsiliste turvaintsidentidega, näiteks nagu volitamata sisenemine ruumidesse või territooriumile, vandalism, vargus, tulekahju või isiku ründamine. Seoses

¹⁹⁶ Andmekaitse Inspeksioon, lk 68.

¹⁹⁷ European Data Protection Supervisor. Video-surveillance Guidelines, lk 18.

¹⁹⁸ Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context, lk 4.

¹⁹⁹ European Data Protection Supervisor. Video-surveillance Guidelines, lk 23.

²⁰⁰ Article 29 Data Protection Working Party. Working document on the Processing of Personal Data by means of Video Surveillance, lk 22.

liigse sekkumisega privaatsusesse ei ole helisalvestamine turvakaameratega põhimõtteliselt üldse õigustatud.²⁰¹

Soomes võib tööandja kasutada jälgimisseadmeid eesmärgiga tagada töötajate ja teiste isikute turvalisus, kaitsta omandit, teostada tootmisprotsesside üle järelevalvet ning ennetada või uurida olukordi, mis ohustavad turvalisust, omandit või tootmisprotsessi. Turvakaameraid ei tohi kasutada konkreetse töötaja või töötajate jälgimiseks. Samas võib tööandja turvakaameraga jälgida konkreetset töökohta, kui see on vajalik ennetamiseks ilmsel ohtu töötajate ohutusele ja tervisele, ennetamiseks ja uurimaks varaga seotud kuritegusid, kui töötajate põhiline osa tööst kujutab endast tegelemist hinnaliste väärtustega, nagu raha, väärtpaberid ja väärisesemed. Samuti kaitsmaks töötaja õigusi ja huve, kui jälgimine toimub jälgitava töötaja palvel ning see on töötaja ja tööandja vahel kokku lepitud.²⁰²

Jälgida ei tohi ruume, mis ei ole mõeldud tööülesannete täitmiseks, vaid töötajate eraviisiliseks kasutamiseks – näiteks tualettruumid, duširuumid, riietusruumid, töötajateapid ja puhkeala.²⁰³ Kabinettide osas on töötajatel samasugune kõrgendatud ootus privaatsusele kui puhkeruumi, tualettruumi ning riietusruumi puhul. Seejuures tuleb kabinetiks lugeda ka ruum, mida jagavad mitu töötajat ning „kuubikuteks“ jagatud suured avatud kontoriruumid.²⁰⁴

Kui töötajate jälgimine on lubatud ja selle vajalikkus on piisavalt põhjendatud, siis tuleb lähtuvalt IKS § 6 p-s 7 sätestatud individuaalse osaluse põhimõttest, samuti tulenevalt IKS § 14 lg-st 3 ja § 15 lg-st 1 jälgimisest töötajaid kindlasti teavitada. Töötajate varjatud jälgimine ei ole lubatud. Teavitama peab töötajaid ka juhul, kui jälgimisseadmed on suunatud klientide või kolmandate isikute jälgimisele, kuid paratamatult jäävad ka töötajad jälgimisalasse. Samuti tuleb jälgimisest teavitada kõiki kolmandaid isikuid, kes satuvad töötajate jälgimiseks üles seatud jälgimisseadmete alla.²⁰⁵

Jälgitavatele peab teatavaks tegema nii jälgimise fakti kui ka jälgimise eesmärgi, samuti ka muud andmed, mis tagavad, et andmete töötlemine oleks andmesubjekti suhtes õiglane, nagu näiteks millisel juhul vaatab salvestisi ettevõtte juhtkond ning millal antakse salvestised üle õiguskaitseorganitele. Jälgimisseadme täpset asukohta ei pea avaldama, kuid jälgimise

²⁰¹ European Data Protection Supervisor. Video-surveillance Guidelines, lk 21–22, 32.

²⁰² Act on the Protection of Privacy in Working Life, section 16.

²⁰³ Article 29 Data Protection Working Party. Working document on the Processing of Personal Data by means of Video Surveillance, lk 22.

²⁰⁴ European Data Protection Supervisor. Video-surveillance Guidelines, lk 29.

²⁰⁵ Andmekaitse Inspeksioon, lk 71.

konteksti peab selgitama üheselt mõistetavalt. Teavitus ei tohi olla paigutatud jälgimisalast ebamõistlikult kaugemale.²⁰⁶

Andmekaitse Inspeksioon soovitab tööandjatel koostada jälgimisseadmete kasutamise kirjelduse, milles oleks ära toodud jälgimisseadmete kasutamise eesmärgid, kas ja milliste töökohustuste rikkumiste menetlemiseks jälgimisseadmete salvestisi võidakse kasutada, jälgitav ala, jälgimise aeg, jälgimise liik (reaalajas või salvestamisega), jälgimisseadmete üldine kirjeldus, jälgimisega kogutud andmete töötleja andmed, jälgimisega kogutud andmete kolmandatele isikutele edastamine, jälgimisega kogutud andmete kaitse korraldus, salvestiste säilitamise aeg ja salvestistega tutvumise kord.²⁰⁷

Jälgimisseadmete kasutamisel tuleb otsustada ka seda, kas on vajalik, et jälgimisseadmed salvestaksid toimuvat või piisab ainult reaalajas jälgimise võimalusest. Kui salvestamist peetakse vajalikuks, tuleb kehtestada kindel periood, mille jooksul salvestisi säilitatakse ja tagada, et peale seda salvestised kustutatakse. Salvestisi ei tohi säilitada kauem kui on vajalik eesmärgi saavutamiseks, milleks need tehti. Kui jälgimisseadmete abil on salvestatud teatud intsident, mille uurimiseks või tõendamiseks on salvestist vaja säilitada kauem kui tavaline säilitusperiood, siis võib seda teha seni, kuni see on uurimise või tõendamise huvides vajalik, kuid peale seda tuleb ka need salvestised kustutada. Euroopa Andmekaitseinspektori hinnangul on turvakaamerate salvestiste mõistlik säilitusperiood üks nädal, sest see aeg peaks olema piisav otsustamiseks, kas salvestist on vaja mingi juhtumi uurimiseks või tõendamiseks.²⁰⁸ Samas turvateenuseid osutav ettevõtte peab arvestama turvaseaduse § 11 lg-ga 4, mille kohaselt säilitatakse jälgimisseadmetiku salvestist vähemalt üks kuu salvestamise päevast arvates, kuid mitte kauem kui üks aasta.

Soomes võib tööandja turvakaamerate salvestisi säilitada üldjuhul maksimaalselt ühe aasta. Samuti peab tööandja tagama selle, et salvestisi kasutatakse ainult sellele eesmärgil, mis oli jälgimise aluseks. Sõltumata jälgimise eesmärgist on tööandjal õigus kasutada salvestisi ka töösuhte lõpetamise aluse tõendamiseks, ahistamise ja kiusamise tõendamiseks ja uurimiseks ning tööõnnetuse uurimiseks.²⁰⁹

²⁰⁶ Article 29 Data Protection Working Party. Working document on the Processing of Personal Data by means of Video Surveillance, lk 19, 22.

²⁰⁷ Andmekaitse Inspeksioon, lk 72.

²⁰⁸ European Data Protection Supervisor. Video-surveillance Guidelines, lk 33.

²⁰⁹ Act on the Protection of Privacy in Working Life, section 17.

Nagu ka kõikidel teistel isikuandmete töötlemise juhtudel, on töötajal õigus tutvuda ka jälgimisseadmete abil tema kohta kogutud andmetega, sealhulgas salvestistega. Töötaja võib paluda endale ka koopia väljastamist, kuid IKS § 19 lg 2 kohaselt väljastatakse isikuandmed andmesubjekti poolt soovitud viisil siiski vaid võimaluse korral. Andmetega tutvumise ja neist koopiate saamise õigus on töötajal sõltumata sellest, kes andmed on kogunud, kas tööandja ise või tema poolt palgatud turvaettevõtte.²¹⁰

Salvestisega tutvumise võimaldamise ning sellest koopia andmise korral tuleb aga arvestada, et salvestis võib sisaldada ka teiste isikute isikuandmeid. Salvestise näitamisest keeldumiseks see siiski alust ei anna – salvestisel tuleb lihtsalt kolmandad isikud muuta tuvastamatuks. Sõltuvalt asjaoludest võib kolmandate isikute identifitseerimatuks muutmine salvestise töötajale näitamise korral olla mittevajalik. Näiteks kolleegide näokujutiste kinnikatmisel või hääle moonutamisel ei ole mõtet, sest töötaja, kes salvestisel kajastatud olukorras ise viibis, tunneks nad nii või teisiti ära. Kui salvestis aga kajastab töötajale teadmata kolmandate isikute andmeid, tuleks need siiski ka salvestise näitamisel tuvastamatuks muuta, v.a juhul, kui tööandja kasutab salvestist töötaja vastu nõude esitamisel tõendina. Töötajale salvestisest koopia andmisel tuleks siiski kõik kolmandad isikud muuta tuvastamatuks, sest koopia väljastamisel ei saa ega pea tööandja kontrollima, mida töötaja selle koopiaga edasi teeb. Kui tööandja on koopia väljastanud, ilma et selleks oleks seaduslik alus, vastutab tööandja kolmandate isikute ees nende isikuandmete ebaseadusliku väljastamise eest.²¹¹

Seoses infotehnoloogia ning tehnikavaldkonna kiire ja pideva arenguga on töötajate jälgimist ja kontrollimist võimaldavad tehnilised lahendused muutunud tööandjate jaoks järjest kättesaadavamaks. Samas jälgimise järjest lihtsamaks ja odavamaks muutumine ei tohiks olla põhjuseks selle kergekäeliseks kasutamiseks tööandjate poolt. Kui jälgimisseadmete kasutamine on tööandja õiguste ja huvide kaitseks vajalik ning õigustatud, tuleb selliste meetmete rakendamisel arvestada käesolevas peatükis tooduga, et kaitsta töötajaid liigse privaatsusesse sekkumise eest, sest privaatsusõigus ei tähenda ainult kontrolliõiguste endaga seotud informatsiooni üle, vaid see tähendab ka õigust mitte olla pideva jälgimise all ehk õigust olla omaette.

²¹⁰ Andmekaitse Inspeksioon, lk 72.

²¹¹ Andmekaitse Inspeksioon, lk 72.

KOKKUVÕTE

Õigus privaatsusele ehk privaatsusõigus on õigus isiklikule elule. See on õigus ise otsustada, millal, kuidas ja millises ulatuses eraelulist informatsiooni teistega jagada. Õiguslik ootus privaatsusele ei piirdu ainult koduga, vaid töötajal on õigus privaatsusele ka oma töökohal ning tööandja peab sellega arvestama. Seda enam, et tänapäeval on töösuhted ja -korraldus muutunud selliseks, et järjest keerulisem on üheselt eristada tööalast tegevust ning eraelu. Samas ei ole privaatsusõigus absoluutne õigus ja seega võib tööandja õigusliku aluse olemasolul töötaja privaatsusõigust ka töösuhtes piirata. Õigustuse sellele annavad eelkõige tööandja põhiõigused – ettevõtlusvabadus ja omandipõhiõigus, mis kaitsevad tööandja huve tegeleda äritegevusega ja tagada edukas ettevõtte toimimine.

Töötaja peab arvestama, et töösuhte normaalseks toimimiseks on vajalik, et tööandja töötleks töötaja isikuandmeid ja teostaks töötaja üle kontrolli, mis võib kaasa tuua privaatsusõiguse riive. Samas peab tööandja silmas pidama, et ta liigselt ei piiraks töötaja privaatsust ning iga töötaja põhiõiguste riive oleks põhjendatud ja proportsionaalne. Seega seni, kuni isikuandmete töötlemine toimub seadusandja poolt kehtestatud reegleid järgides, on töötaja privaatsusõiguse riive õigustatud. Samas ei ole seadusandja töötaja privaatsusõiguse piiramist, sealhulgas antud magistr töö teemaks olevat töötaja kontrollimist ja jälgimist, töösuhetes eraldi õigusaktiga reguleerinud, vaid lähtuda tuleb üldistest andmekaitse põhimõtetest.

Andmekaitse Inspeksioon on teema selgitamiseks välja andnud abistava juhendmaterjali, milles on väga põhjalikult käsitletud isikuandmete töötlemist töösuhetes. Juhises on ühendatud nii andmekaitse teooria kui ka praktika, analüüsitud on asjakohaseid põhiõigusi ning nende riivet, kuid samas on pakutud välja ka praktilisi juhiseid võimalike probleemsete olukordade lahendamiseks. Kohati võib see juhendmaterjal olla keskmise tööandja jaoks liigagi põhjalik ja andmekaitse teooriasse süvitsi minev. Arvestades töösuhte erilist iseloomu, teema delikaatsust ja seda, et see puudutab peaaegu kõiki tööealisi inimesi, võib jääda sellest soovituslikust juhiseist väheseks. Seda enam, et infotehnoloogia arenedes avarduvad ja lihtsustuvad ka võimalused kontrolli ja jälgimise teostamiseks.

Tagamaks töösuhte poolte õiguskindlust, peaks töötajate kontrollimine ja jälgimine töösuhtes olema seadusandja poolt reguleeritud nii, et töötajatel oleks selge ja ühene arusaamine, millal ja kuidas tööandja teda jälgida ja kontrollida võib ning tööandjatel konkreetne ülevaade, millistel tingimustel ja ulatuses ta seda teha tohib. Selle probleemi lahendamiseks tuleks need

küsimused seadusandja poolt õigusaktiga reguleerida. Samuti on uues isikuandmete kaitse üldmääruse eelnõus liikmesriikidele antud volitus võtta vastu kooskõlas nimetud määrusega õigusakte reguleerimaks isikuandmete töötlemist töösuhetes.

Üks võimalus on reguleerida need küsimused eraldi õigusaktiga, nagu seda on tehtud Soomes. Lähtudes aga asjaolust, et töösuhet puudutavad olulised normid võiksid olla koondatud ühte seadusesse, kuna see lihtsustab nende kättesaadavust töösuhte osapoolte jaoks, oleks autori arvates mõistlikum lisada vastavad sätted töölepingu seadusesse. See peaks parandama ka töösuhte poolte teadlikkust oma õigustest ja kohustustest. Samas ei peaks neid küsimusi seaduses reguleerima peensusteni, sest liiga detailsed sätted võivad osutuda kokkuvõttes ebapiisavaks, kuna kõiki olukordi pole kindlasti võimalik ette näha. Pigem peaks seadusandja kehtestama üldise korra töötaja privaatsusõiguse piiramiseks ning tööandjale kohustuse reguleerida sellised küsimused täpsemalt ettevõttesiseselt. Seadusandja poolt kehtestatud korraga peaks sätestama töötaja privaatsusõiguse piiramise üldised tingimused ja ulatuse ning andma tööandjale juhised ettevõttesiseste reeglite kehtestamiseks.

Kuna tööandjate tegevusalad on väga erinevad, siis sellest tulenevalt erinevad ka töötaja privaatsusõigust puudutavad reguleerimist vajavad küsimused. Seega suudavad tööandjad ise kõige paremini võimalikke probleemkohti ette näha ning neid küsimusi reguleerida nii detailselt kui probleemide ennetamiseks ja lahendamiseks vajalik ning võimalik. Sellise korra võib kehtestada eraldi ettevõttesisese privaatsuspoliitikana või lisada need sätted töökorralduse reeglitesse. Oluline on, et tööandja kehtestatud reegleid töötajatele tutvustaks ja vajadusel selgitaks, nii et mõlemal töösuhte poolel oleks ühesugune ja selge arusaamine oma õigustest ja kohustustest, mis seostuvad privaatsusõiguse ja selle võimaliku piiramisega.

Praegusel hetkel seadus otseselt tööandjatele ettevõttesisese privaatsuspoliitika koostamise kohustust ette ei näe, kuid kui tööandja soovib töötaja privaatsusõigust piirata – jälgida ja kontrollida töötaja kommunikatsioonivahendite kasutamist või kasutada erinevaid jälgimisseadmeid, siis ilma vastavate reeglite kehtestamiseta ja töötajate teavitamiseta, ei ole selline töötajate jälgimine lubatud. Edumeelsed tööandjad on probleemide ennetamiseks lisanud töölepingusse kokkuleppe, et tööandjal on õigus jälgida tööandja poolt töötaja kasutusse antud kommunikatsioonivahendite sihtotstarbelist kasutamist. Vahel võib see olla sõlmitud ka eraldi kokkuleppena või on lisatud vastavad sätted töökorralduse reeglitesse.

Samas seni, kuni selliste reeglite koostamine ja kokkulepete sõlmimine on vabatahtlik ja soovituslik, siis ei pruugi tööandjad seda ebavajalikuks pidades, lihtsalt teadmatusest või mingil muul põhjusel kehtestada. See ei tähenda aga seda, et kontrolli ja jälgimist ilma vastava töötajate teavitamiseta läbi ei viidaks. Tagajärjeks on see, et tegelikult ei ole piisavalt kaitstud töötajate privaatsus, kuna töötajad ei pruugi olla teadlikud tööandjapoolsest jälgimisest ja selle ulatusest, ega ka tööandja, kel puudub õiguslik alus sellise jälgimise ja kontrollimise käigus tuvastatud töötaja rikkumistele reageerida omapoolsete sanktsioonidega. Vaatamata sellele, et ei ole olemas sellist üldist õigust, mis annaks töötajale õiguse kasutada tööandja kommunikatsioonivahendeid isiklikuks otstarbeks, siis ilma reeglite kehtestamiseta on töötajal õiguspärane ootus privaatsusele ning tööandja poolt jälgimise ja kontrollimisega töötaja privaatsusse sekkumine ning privaatsusõiguse riive ei ole õigustatud.

Kui tööandja töötajat võimalikust jälgimisest ja kontrollimisest teavitab, siis töötaja ootused privaatsusele vähenevad. Ettevõttesisese privaatsuspoliitika koostamisel tuleb arvestada vastanduvate tööandja ja töötaja õigustega ning leida lahendus, mis mõlemaid pooli rahuldaks ja nende huvide kaitse tagaks. Kommunikatsioonivahendite kasutamise reeglites peab tööandja selgelt sätestama, kuidas on töötajal lubatud sidevahendeid kasutada, kas neid võib kasutada ka isiklikul otstarbel, kas ja kuidas tööandja kommunikatsioonivahendite kasutamist kontrollib ja jälgib ning millised on eeskirjade rikkumise tagajärjed.

Võimalusi töötajate jälgimiseks ja kontrollimiseks on palju ning seoses infotehnoloogia arenguga tuleb neid järjest juurde, kuid ainuüksi kontrollimist ja jälgimist võimaldavate lahenduste kättesaadavaks muutumine ei õigusta nende kasutamist tööandja poolt. Igasugune kontroll- või jälgimismeetodi kasutamine tööandja poolt peab olema põhjendatud ning sellega kaasnev võimalik töötaja privaatsusõiguse riive peab olema soovitava eesmärgiga proportsionaalne. Seega tasuks näiteks tööandjal töötajate kontrollimise meetodite valimisel kaaluda, kas elektrooniliste jälgimisseadmete asemel ei õnnestuks sama tulemust saavutada ettevõtte juhtimis- ja töötajate juhendamise süsteemi täiustades või selle asemel, et jälgida ja kontrollida kõik töötajaid, võiks keskenduda nendele, kelle suhtes on tööandjal kahtlused või kelle kohta on esitatud tööandjale kaebusi.

Tööandja peab arvestama ka sellega, et töötaja liigne kontrollimine ja jälgimine võib põhjustada töötajas usaldamatust tööandja vastu ning tööülesannete parema täitmise asemel tuua kaasa hoopis vastupidise tulemuse ja halvendada töösuhte toimimist. Kuna hästitoimiva töösuhte oluliseks eelduseks on poolte õiguste ja huvide vastastikune austamine.

Kui töötaja privaatsusõiguse piiramine pole seadusandja poolt piisavalt reguleeritud ja piirangute ulatus ning rakendamise tingimused on jäetud ainult tööandja otsustada, võib see kujutada ohtu töötaja privaatsusõigusele üldisemas plaanis. Nimelt ei pruugi tööandjad reegleid kehtestades arvestada oma ettevõtte ja töötajate töö eripäraga, vaid võivad hakata oma huvide kaitseks igaks juhuks ettevõttesiseste dokumentidega töötajate privaatsusõigust võimalikult palju piirama, nähes ette ka sellist töötaja jälgimist ja kontrollimist, mis ei tarvitse konkreetses ettevõttes olla üldse põhjendatud ega vajalik. Kui töötaja soovib konkreetse tööandja juures töötada, siis üldjuhul peab ta ka nõustuma selle tööandja poolt kehtestatud reeglitega ja neid järgima. Antud juhul tähendaks töötaja nõustumine tööandja poolt kehtestatud ebamõistliku jälgimise ja kontrollimise korraga töötaja loobumist suures osas oma õigusest privaatsusele. See võib kaasa tuua selliste töötaja privaatsust liigselt piiravate tingimuste muutumise standardpunktideks tööandja töökorralduse reeglites, mis omakorda mõjutab negatiivselt ühiskonna üldist töötaja privaatsusõiguse aktsepteerimist töökohal.

Kokkuvõtteks võib järeldada, et püstitatud hüpotees leidis osaliselt kinnitust. Hetkel on läbi isikuandmete töötlemise üldiste reeglite ja põhimõtete teatud määral töötaja ja tööandja põhiõiguste kaitse küll tagatud, kuid selline regulatsioon on töösuhetes töötajate jälgimisel ja kontrollimisel rakendamiseks liiga üldine ning ei ole töösuhete poolte jaoks piisavalt selge ega arusaadav. Sellest tulenevalt ei täida kehtiv õiguslik regulatsioon soovitud eesmärki töösuhete poolte põhiõiguste kaitsmisel. Konkreetsed õigusaktiga kehtestatud reeglid töösuhetes privaatsuse piiramiseks tõhustaksid tunduvalt poolte õiguste ja huvide kaitset. Seega autori arvates ei taga hetkel kehtiv töötaja privaatsusõiguse piiramist töösuhetes puudutav õiguslik regulatsioon töötaja ega tööandja põhiseaduses sätestatud õiguste tõhusat kaitset.

Kuigi infotehnoloogia areng ja interneti avarad võimalused on mõnevõrra mõjutanud ka privaatsuse tähendust ühiskonnas, ei ole see vähendanud töötajate ootust ja õigust privaatsusele töökohas. Samas on tööandjal töösuhetega seoses omad eesmärgid ja huvid, mida ei ole võimalik saavutada ega kaitsta ilma omamata piisavat kontrolli töötajate üle. Seadusandja ülesandeks ongi leida tasakaal töösuhete poolte õiguste ja huvide vahel, sätestades õigusaktiga korra, mis kaitseks nii töötajat liigse privaatsusõigusesse sekkumise eest kui ka tagaks tööandja majanduslike huvide kaitset.

EMPLOYEE'S RIGHT TO PRIVACY AND ITS RESTRICTION IN LABOUR RELATIONS

SUMMARY

The right to privacy is a right to private life. This is the right to decide on your own when, how and to which extent to share private information with other people. The legitimate expectation of privacy is not limited to one's home, the employee has the right to privacy also at work and the employer must take it into account. At the same time the right to privacy is not an absolute right and therefore the employer may restrict it in business relations if there is legal ground for it. This is justified primarily by the employer's fundamental rights – freedom of enterprise and the fundamental right to property that protect the employer's interests to be engaged in business and guarantee successful functioning of the enterprise. The employee has the right to protect his privacy, but at the same time the employer has the right to protect his economic interests.

The given Master's thesis deals with the employee's right to privacy and its restriction in labour relations primarily by supervising the employee and his usage of means of communication that in certain cases may seriously infringe on the employee's right to privacy. According to § 1 of the Employment Contracts Act the employee is subordinated to the management and supervising control of the employer. At the same time it should be done respecting employee's privacy and not violating his fundamental rights. The aim of the given thesis is to make clear in which cases, to what extent and how the employer may restrict the employee's right to privacy – for example record the phone calls, read the employee's e-mails, control the employee's computer usage, film the employees with security cameras or supervise them by other methods, and whether such supervising control and surveillance should be regulated more precisely by legislator.

At present there is no concrete legal regulation concerning the restriction of employees' right to privacy in Estonia, as there is no special act that would regulate data protection in labour relations. Therefore it is necessary to proceed in these questions from general principles of the processing and protecting of personal data that are enacted in the Personal Data Protection Act. In addition, the Data Protection Inspectorate issued advisory instructions, Processing of Personal Data in Labour Relations, at the beginning of 2011. In the given thesis an attempt is made to get a clear idea if such instructions are sufficient to regulate supervising control and

surveillance of the employees in labour relations and whether it protects employees from excessive interference in their privacy, at the same time guaranteeing the protection of employer's economic interests.

The relevant juridical literature, legal acts, juridical practice and directions for employers for supervising employees given in the instructions of the Data Protection Inspectorate have been analysed in this thesis in order to find answers to the questions raised. Since respective juridical practice has not yet been established in Estonia, the thesis concentrates primarily on the juridical practice of European Court of Human Rights. As the restriction of the employee's privacy in labour relations is regulated differently in different countries and there is no uniquely fixed standpoint, the examples of respective legislation and established practice of Great Britain and Finland in this sphere are given to have a better survey of the subject.

In the first chapter of the thesis the concept of privacy, right to privacy and its protection sphere are defined. In this connection fundamental rights relating to the employee's right to privacy (such as right to privacy, right to confidentiality of messages, right to free self-realization and right to freedom of expression) are dealt with. It is also analysed if and on what conditions infringement of these fundamental rights is justified. In addition, this chapter also deals with the fundamental rights of the employer that in labour relations contradict the employee's fundamental rights since on the basis of these fundamental rights of the employer in certain cases he has the right to invade the privacy of the employee to protect his fundamental rights.

The second chapter concentrates on the rules and principles of the data protection since the data protection has a very essential role in the implementation of the right to privacy. This chapter clarifies the fundamental concepts of the processing of personal data. The general principles and legal ground of the processing of personal data are also dealt with. Since personal data are processed also in the course of employer's supervisory control and surveillance, these rules must be followed while doing it. In addition, this chapter discusses the liability of the employer for the processing of personal data or what sanctions the violation of the principles of the processing of personal data can bring about to the employer.

The third chapter deals with the restriction of the employee's privacy by the employer by using supervisory control of the means of communication and surveillance devices. Employer's rights and possibilities to supervise the employee are analysed. An attempt is also

made to find the answer to the question if and to what extent the employee has the right to use the means of communication given by the employer for personal purposes. Circumstances under which the employer has the right to supervise the employees' use of the means of communication are brought out. The use of the surveillance devices is also dealt with, in which cases such surveillance is justified and permitted, what conditions must be fulfilled in every concrete case and to what extent the employer may do that.

The employee must take into consideration that for the normal functioning of the employment relationship it is necessary that the employer processes the personal data of the employee and supervises the employee which may bring about certain infringement of privacy rights. But at the same time the employer must keep it in mind that he would not excessively restrict the employee's privacy and the infringement of the fundamental rights of every employee would be justified and proportional. Accordingly, the infringement of privacy rights of the employee is justified as long as the rules established by legislator have been followed in processing personal data.

Today legislator has not regulated by any separate legislation the restriction of the right to privacy in labour relations, including the supervisory control and surveillance of the employee that is the theme of the given thesis. One has to follow the general principles of data protection. The Data Protection Inspectorate has issued advisory instructions to clarify the matter, but this may be insufficient considering the special nature of the employment relationship, the sensitivity of the matter and the fact that it concerns almost all people of working age. Moreover, the development of info technology enables to widen and simplify the control and surveillance. To guarantee the legal certainty of the parties in labour relations the supervisory control and surveillance of the employees should be regulated by legislator so that the employees understand clearly and unambiguously when and how the employer may supervise them and the employers have a concrete survey on what conditions and to what extent they have right to do that.

One possibility is to regulate these matters in detail by separate legislation. But proceeding from the fact that the significant rules regarding the labour relations would be concentrated in one act of law to make them more accessible to the parties of the labour relations, the author thinks it more reasonable to add these provisions to the Employment Contracts Act.

At the same time these questions must not be regulated in detail, because too much detailed provisions may prove to be insufficient since it is certainly impossible to foresee all situations. Rather, the legislator should establish general rules for the restriction of the employee's right to privacy and the obligation for the employer to regulate such matters more precisely in the enterprise. The rules established by the legislator should enact the general conditions and extent of the restriction of employee's right to privacy and give the employer instructions for imposing more exact regulations.

As the activities of the employers differ considerably, they themselves can foresee the problems best of all and regulate these matters as thoroughly as it is possible and necessary to prevent and solve the problems. Such rules can be established separately as the privacy policy within the enterprise or add these provisions to the rules of the organization. Drawing up the privacy policy of the enterprise, the opposite rights of the employer and the employee must be taken into account and the solution found which satisfies both parties and guarantees the protection of their interests. In the rules concerning the use of the means of communication the employer must clearly establish how the employee is allowed to use the means of communication, whether they may also be used for personal purposes, if and how the employer controls the use of the means of communication and what the consequences of the violation of the rules are.

At present the legislation does not foresee directly the obligation for employers to draw up the privacy policy in the enterprise, but if the employer wishes to restrict the employee's right to privacy – to supervise and control the use of the means of communication by the employee or use different surveillance devices - such supervision is not permitted without establishing relevant rules and informing the employees. But then, as long as the drawing up such rules is voluntary and of advisory nature, the employers may not establish them. That does not mean that the employees will not be controlled and supervised without informing. The result is that neither the employees' privacy who may not be aware of being supervised by the employer is sufficiently protected nor the employer's privacy who has no legal ground to respond with sanctions to the employee's offences ascertained by supervisory control.

There are many possibilities to control and supervise the employees and more are being added by the development of info technology, but the availability of these technological solutions does not justify using them by employer. Any use of methods of control or surveillance by the employer must be justified and the potential related infringement of the employee's privacy

rights must be proportional to the expected aim. The employer must also take into account that excessive control and surveillance may cause the employee's mistrusting the employer and instead of better task fulfillment may bring about negative result and impair the functioning of the employment relationship. The significant precondition of the well-functioning employment relationship is the mutual respect for the rights and interests of both parties.

If the restriction of the employee's privacy rights is not sufficiently regulated by the legislator and the extent of restrictions and terms of their implementation are left solely to the employer to decide it may be a danger to the employee's privacy rights on a more general ground. The employers may not take into account the speciality of their enterprise and the employees' work. To protect their rights they may begin to restrict the employees' privacy rights as much as possible by in-house acts. These restrictions may include such control and surveillance of the employee that may not be grounded or necessary in this enterprise. It may bring about a situation when such excessive restrictions of the employee's privacy turn into standard articles in the employer's rules of management. That has a negative influence on the general acceptance of the employee's privacy rights at work by the society.

In conclusion it can be said that the employees and employers fundamental rights are currently ensured to some extent through the general rules and principles of the personal data processing, but such regulation is too general for implementing in labour relations for the employees surveillance and control purposes. In addition, this regulation isn't sufficiently explicit nor understandable for the labor relations parties. Consequently, the current legal regulation fails to comply with the goal of protecting the rights of the labour relation parties. Specific rules on restriction of privacy in labour relations established by legislation would intensify the protection of the rights and the interests of the employees and employers. Therefore, it can be stated that the current legislation on restriction of employee's right to privacy in labor relations does not ensure effective protection of employees and employers fundamental rights.

Though the development of the info technology and the ample facilities of the internet have to some extent influenced the meaning of privacy in the society that has not diminished the employees' expectations and right to privacy at work. At the same time, the employer has his expectations and interests concerning the labour relations that are not possible to be achieved or protected without sufficient control over the employee. The task of the legislator is to find

balance between the rights and interests of the parties of labour relations, enacting the rules that protect the employee from the excessive interference in the privacy rights and ensure the protection of the employer's economic interests as well.

.....

04.05.2012

KASUTATUD LÜHENDID

AKI juhis – Andmekaitse Inspektsiooni abistav juhendmaterjal „Isikuandmete töötlemine töösuhetes“

Andmekaitse direktiiv – Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta

EIK – Euroopa Inimõiguste Kohus

EIOK – Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni

Euroopa andmekaitseasutuste tööühik – Andmekaitse direktiivi artikkel 29 alusel Euroopa Liidu liikmesriikide andmekaitseasutuste esindajatest moodustatud tööühik, mis analüüsib andmekaitse direktiivi rakendamist liikmesriikides ning annab soovitusi ja hinnanguid andmekaitse direktiivi kohaseks rakendamiseks.

IKS – Isikuandmete kaitse seadus

ILO – Rahvusvaheline Tööorganisatsioon

KarS – Karistusseadustik

PS – Eesti Vabariigi põhiseadus

TLS – Töölepingu seadus

TTOS – Töötervishoiu ja tööohutuse seadus

VÕS – Võlaõigusseadus

UK juhis – Information Commissioner's Office „The Employment Practices Code“

KASUTATUD KIRJANDUS

1. Alexy, R. Põhiõigused Eesti põhiseaduses. – Juridica eriväljaanne 2001.
2. Andmekaitse Inspeksioon. Isikuandmete töötlemine töösuhetes. Abistav juhendmaterjal. Tallinn: 2010. Kinnitatud 24.01.2011. Arvutivõrgus: <http://www.aki.ee/download/1818/Isikuandmed%20töösuhetes%20juhendmaterjal%20LÕPLIK.pdf>, 09.01.2012.
3. Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context. Arvutivõrgus: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf>, 03.02.2012.
4. Article 29 Data Protection Working Party. Recommendation 1/2001 on Employee Evaluation Data. Arvutivõrgus: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp42en.pdf>, 03.02.2012.
5. Article 29 Data Protection Working Party. Working document on the Processing of Personal Data by means of Video Surveillance, 2002. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp67_en.pdf, 03.02.2012.
6. Article 29 Data Protection Working Party. Working document on the surveillance of electronic communications in the workplace, 2002. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf, 03.02.2012.
7. Artikli 29 alusel loodud andmekaitse töörühm. Arvamus 4/2007 isikuandmete mõiste kohta. Arvutivõrgus: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_et.pdf, 03.02.2012.
8. Buitelaar, J. C. Privacy: Back to the Roots. – German Law Journal 2012/13, No 3.
9. Council of Europe Committee of Ministers. Recommendation No. R (89) 2 on the protection of personal data used for employment purposes. Arvutivõrgus: <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276592&SecMode=1&DocId=699842&Usage=2>, 20.02.2012.
10. Dowding, M. R. Privacy: Defending an Illusion. Plymouth: Scarecrow Press 2011.
11. European Data Protection Supervisor. Video-surveillance Guidelines, 2010. Arvutivõrgus: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf, 01.02.2012.
12. Filippov, M. Andmekaitse: tööalane ja erakirjavahetus olgu lahus. – Postimees 29.11.2011. Arvutivõrgus: <http://www.postimees.ee/651268/andmekaitse-tooalane-ja-erakirjavahetus-olgu-lahus/>, 27.02.2012.

13. Haigekassa THV maksmise kord: küsimused ja vastused. Arvutivõrgus:
<http://www.haigekassa.ee/tooandjale/tvh-maksmise-kord-kysimu>, 12.02.2012.
14. Henberg, A. Isikuandmete töötlemine töösuhetes. – Juridica 2005/8.
15. Ilus, T. Andmesubjekti osaluse põhimõtte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. – Juridica 2005/8.
16. Information Commissioner's Office. The Employment Practices Code, 2011. Arvutivõrgus:
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/employment.aspx, 23.01.2012.
17. Information Commissioner's Office. The Employment Practices Code. Supplementary Guidance, 2005. Arvutivõrgus:
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/employment.aspx, 20.02.2012.
18. Jõks, A. Eraelu kaitse töösuhetes – väljakutse tööandjale. Ettekanne Andmekaitse inspeksiooni konverentsil, 27.01.2010. Arvutivõrgus:
[http://www.aki.ee/download/1480/allarj%20270110%20%20PPT\(1733968_1\)%20ettekanne%20%20\[Kirjutuskaitstud\].pdf](http://www.aki.ee/download/1480/allarj%20270110%20%20PPT(1733968_1)%20ettekanne%20%20[Kirjutuskaitstud].pdf), 19.02.2012.
19. Kuner, C. European Data Protection Law: Corporate Compliance and Regulation. Oxford; New York: Oxford University Press 2007.
20. Lugaresi, N. Electronic privacy in the workplace: Transparency and responsibility. – International review of Law, Computers & Technology 2010/24, No 2.
21. Maruste, R. Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn: Juura 2004.
22. Michael, J. Privacy and human rights: an international and comparative study, with special reference to developments in information technology. Paris: UNESCO Publishing 1994.
23. Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011.
24. Nouwt, S., De Vries, B. R., Prins, C. Reasonable Expectations of Privacy? The Hague: T.M.C. Asser Press 2005.
25. Nõmper, A., Michelson, K. Kas tööandja saab sidevahendite kasutamist kontrollida? Arvutivõrgus: <http://www.e24.ee/240487/kas-tooandja-saab-sidevahendite-kasutamist-kontrollida/>, 19.02.2011.
26. Palm, E. Privacy Expectation at Work – What is Reasonable and Why? – Ethic Theory Moral Practice 2009/12, No 2.
27. Pikamäe, P., Sootak, J. Karistusseadustik: kommenteeritud väljaanne. Tallinn: Juura 2009.
28. Pilving, I. Õigus isikuandmete kaitsele. – Juridica 2005/7.

29. Seletuskiri Euroopa Parlamendi ja nõukogu määruse eelnõu üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. Arvutivõrgus: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_et.pdf, 01.04.2012.
30. Seletuskiri töölepingu seaduse eelnõu juurde. Arvutivõrgus: http://www.riigikogu.ee/?page=en_vaade&op=ems&eid=353198&u=20090309131308, 06.02.2012.
31. Tikk, E., Nõmper, A. Informatsioon ja õigus. Tallinn: Juura 2007.
32. Truuväli, E.-J. jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Tallinn: Juura 2008.
33. Tööinspektsiooni juhend – Töötaja omavastutus – kas lubada või mitte? Arvutivõrgus: [http://www.ti.ee/public/files/Tootaja%20omavastutus\(1\).pdf](http://www.ti.ee/public/files/Tootaja%20omavastutus(1).pdf), 22.01.2012
34. Töösuhete käsiraamat. Tallinn: Äripäeva Kirjastus 2011.
35. Warren, S. D., Brandies, L. D. The Right to Privacy. – Harvard Law Review 1890/5.
36. Wildhaber, L., Diggelmann, O. Euroopa inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. – Juridica 2007/1.
37. Willborn, S. L. Consenting Employees: Workplace Privacy and the Role of Consent. – Louisiana Law Review 2006/66.

KASUTATUD ÕIGUSAKTID

38. Act on the Protection of Privacy in Electronic Communications. Arvutivõrgus: <http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf>, 22.02.2012.
39. Act on the Protection of Privacy in Working Life. Arvutivõrgus: <http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf>, 22.02.2012.
40. Avaliku teenistuse seadus. – RT I 1995, 16, 228 ... RT I, 29.12.2011, 166.
41. Eesti Haigekassa seadus. – RT I 2000, 57, 374 ... RT I, 23.12.2011, 7.
42. Eesti Vabariigi põhiseadus. – RT 1992, 26, 349 ... RT I, 27.04.2011, 2.
43. Euroopa Liidu põhiõiguste harta. – ELT eestikeelne väljaanne C 83, 30.03.2010, lk 389–403.
44. Euroopa Liidu toimimise leping. – ELT eestikeelne väljaanne C 83, 30.03.2010, lk 47–199.
45. Euroopa Parlamendi ja Nõukogu 24.10.1995.a direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – EÜT L 281, 23.11.1995, lk 31–50 (eestikeelne eriväljaanne: ptk 13, kd 015, lk 355–374).
46. Inimõiguste ja põhivabaduste kaitse konventsioon. 04.11.1950. – RT II 2010, 14, 54.
47. Isikuandmete kaitse seadus. – RT I 2007, 24, 127 ... RT I, 30.12.2010, 11.
48. Karistusseadustik. – RT I 2001, 61, 364 ... RT I, 29.12.2011, 190.
49. Politsei ja piirivalveseadus. – RT I 2009, 26, 159 ... RT I, 29.12.2011, 28.
50. Ravikindlustuse seadus. – RT I 2002, 62, 377 ... RT I, 10.06.2011, 8.
51. The International Labour Office Code of practice on the protection of workers' personal data. Arvutivõrgus: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf, 15.01.2012.
52. Tsiviilkohtumenetluse seadustik. – RT I 2005, 26, 197 ... RT I, 28.12.2011, 44.
53. Turvaseadus. – RT I 2003, 68, 461 ... RT I, 29.12.2011, 51.
54. Töölepingu seadus. – RT I 2009, 5, 35 ... RT I, 10.02.2012, 2.
55. Töötajate tervisekontrolli kord. SoMm 24.04.2003 nr 74. – RTL 2003, 56, 816.
56. Töötervishoiu ja tööohutuse seadus. – RT I 1999, 60, 616 ... RT I, 10.02.2012, 5.
57. Võlaõigusseadus. – RT I 2001, 81, 487 ... RT I, 08.07.2011, 21.
58. ÜRO inimõiguste ülddeklaratsioon. 10.12.1948. Arvutivõrgus: <http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=est>, 12.03.2012.

KASUTATUD KOHTUPRAKTIKA

- 59. EIKo 16.12.1992, 13710/88, *Niemietz vs. Saksamaa*.
- 60. EIKo 25.06.1997, 20605/92, *Halford vs. Ühendkuningriik*.
- 61. EIKo 16.02.2000, 27798/95, *Amann vs. Šveits*.
- 62. EIKo 09.04.2007, 62617/00, *Copland vs. Ühendkuningriik*.
- 63. RKKKo 3-1-1-80-97.
- 64. RKHKo 3-3-1-98-06.
- 65. RKHKo 3-3-1-45-11.